Configurazione di pfSense Community Load Balancer per ECE

Sommario

Introduzione

In questo documento viene descritto come configurare pfSense Community Edition come servizio di bilanciamento del carico per Enterprise Chat and Email (ECE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ECE 12.x
- pfSense Community Edition

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- ECE 12.6(1)
- pfSense Community Edition 2.7.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Installa pfSense

Panoramica della soluzione

pfSense Community Edition è un prodotto multifunzione che fornisce un firewall, un servizio di bilanciamento del carico, uno scanner di sicurezza e molti altri servizi in un unico server. pfSense è costruito su Free BSD e ha requisiti hardware minimi. Il load balancer è un'implementazione di HAProxy ed è disponibile un'interfaccia grafica di facile utilizzo per configurare il prodotto.

È possibile utilizzare questo servizio di bilanciamento del carico sia con ECE che con il portale di gestione del contact center (CCMP). In questo documento viene descritto come configurare pfSense per ECE.

Preparazione

Passaggio 1. Scarica il software pfSense

Utilizzare il sito Web pfSense per scaricare l'immagine del programma di installazione ISO.

Passaggio 2. Configura macchina virtuale

Configurare una VM con i requisiti minimi:

· CPU compatibile con amd64 (x86-64) a 64 bit

· 1 GB o più di RAM

· Unità disco da 8 GB o più (SSD, HDD, ecc.)

· Una o più schede di rete compatibili

· Unità USB avviabile o unità ottica ad alta capacità (DVD o BD) per installazione iniziale

Per un'installazione in laboratorio, è necessaria una sola interfaccia di rete (NIC). L'accessorio può essere eseguito in diversi modi, ma il modo più semplice consiste nell'utilizzare una singola scheda NIC, detta anche modalità a braccio singolo. In modalità one-arm, c'è una singola interfaccia che comunica alla rete. Si tratta di un metodo semplice e adeguato per essere utilizzato in laboratorio, ma non è il più sicuro.

Un modo più sicuro di configurare l'accessorio consiste nel disporre di almeno due schede NIC. Una NIC è l'interfaccia WAN e comunica direttamente con l'Internet pubblico. La seconda scheda NIC è l'interfaccia LAN e comunica con la rete aziendale interna. È inoltre possibile aggiungere ulteriori interfacce per comunicare con diverse parti della rete che hanno regole di sicurezza e firewall diverse. Ad esempio, è possibile avere una scheda NIC connessa alla rete pubblica Internet, una connessa alla rete DMZ in cui si trovano tutti i server Web accessibili esternamente e una terza scheda NIC connessa alla rete aziendale. Ciò consente agli utenti interni ed esterni di accedere in modo sicuro allo stesso set di server Web conservati in una DMZ. Prima dell'implementazione, accertarsi di comprendere le implicazioni di sicurezza di qualsiasi progetto. Consultare un tecnico addetto alla sicurezza per garantire che vengano seguite le best practice per l'implementazione specifica.

Installazione

Passaggio 1. Montare l'ISO sulla VM

Passaggio 2. Accendere la VM e seguire le istruzioni per l'installazione.

Fare riferimento a questo documento per istruzioni dettagliate.

Configurazione della rete

Per continuare la configurazione, è necessario assegnare gli indirizzi IP all'accessorio.

Nota: nel documento viene mostrato un accessorio configurato in modalità monolama.

Passaggio 1. Configurazione delle VLAN

Per il supporto di VLAN, rispondere alla prima domanda con y. In caso contrario, rispondere n.

Passaggio 2. Assegnazione interfaccia WAN

L'interfaccia WAN è il lato non sicuro dell'accessorio in modalità a due bracci e l'unica interfaccia in modalità a un braccio. Quando richiesto, immettere il nome dell'interfaccia.

Passaggio 3. Assegnazione dell'interfaccia LAN

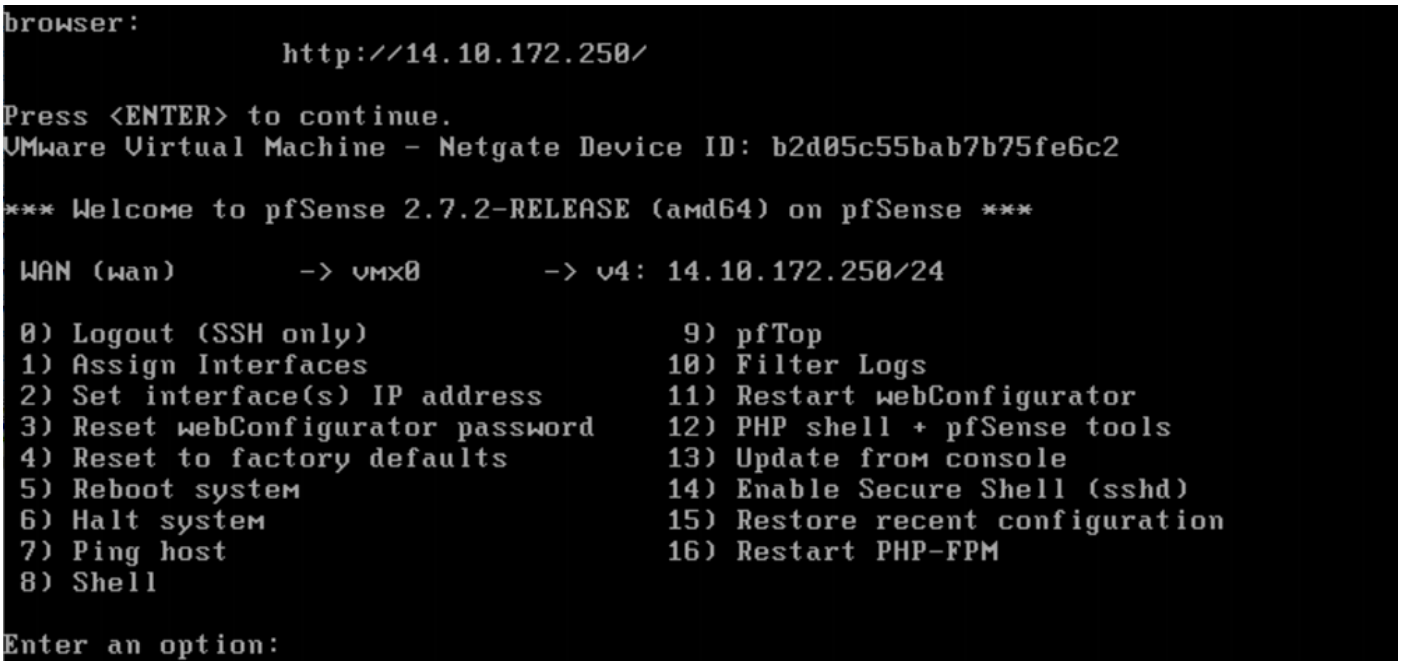
L'interfaccia LAN è il lato sicuro dell'accessorio in modalità a due bracci. Se necessario, immettere il nome dell'interfaccia quando richiesto.

Passaggio 4. Assegnazione di altre interfacce

Configurare tutte le altre interfacce necessarie per l'installazione specifica. Si tratta di opzioni facoltative e non comuni.

Passaggio 5. Assegna indirizzo IP all'interfaccia di gestione

Se la rete supporta DHCP, l'indirizzo IP assegnato verrà visualizzato nella schermata della console.

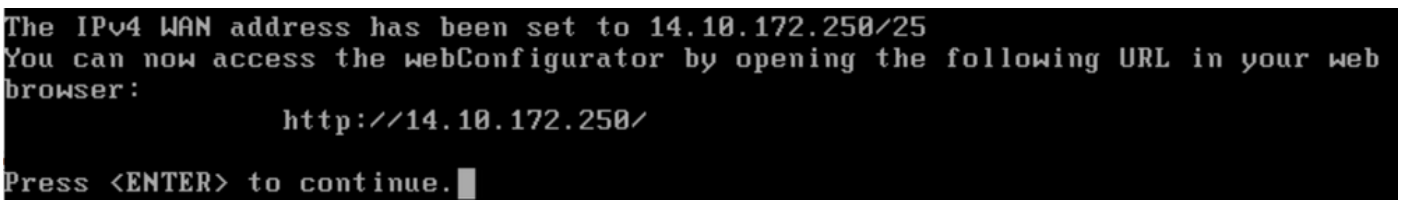


Console pfSense

Se non è stato assegnato alcun indirizzo o se si desidera assegnare un indirizzo specifico, effettuare le seguenti operazioni.

1. Scegliere l'opzione 2 dal menu della console.
2. Rispondere n per disabilitare DHCP.
3. Immettere l'indirizzo IPv4 per l'interfaccia WAN.
4. Immettere la netmask nel numero di bit. (24 = 255.255.255.0, 16 = 255.255.0.0, 8 = 255.0.0)
5. Immettere l'indirizzo del gateway per l'interfaccia WAN.
6. Se si desidera che il gateway sia quello predefinito per l'accessorio, rispondere y al prompt del gateway, altrimenti rispondere n.
7. Se desiderato, configurare la scheda NIC per IPv6.
8. Disabilitare il server DHCP sull'interfaccia.
9. Rispondere y per abilitare HTTP sul protocollo webConfigurator. Questa opzione verrà utilizzata nei passaggi successivi.

Si riceve quindi la conferma che le impostazioni sono state aggiornate.

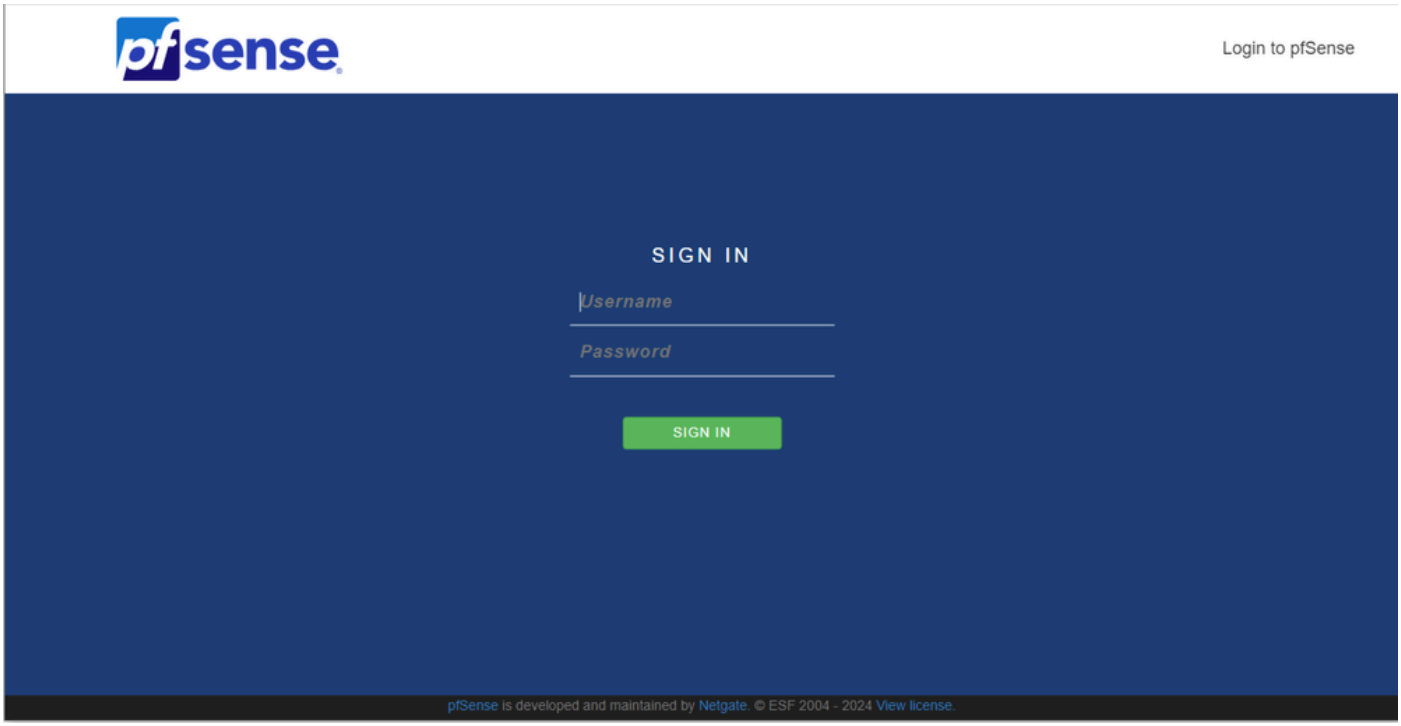


Conferma pfSense

Completa impostazione iniziale

Passaggio 1. Aprire un browser Web e selezionare: http://<indirizzo_ip_accessorio>

Nota: inizialmente è necessario utilizzare HTTP e non HTTPS.

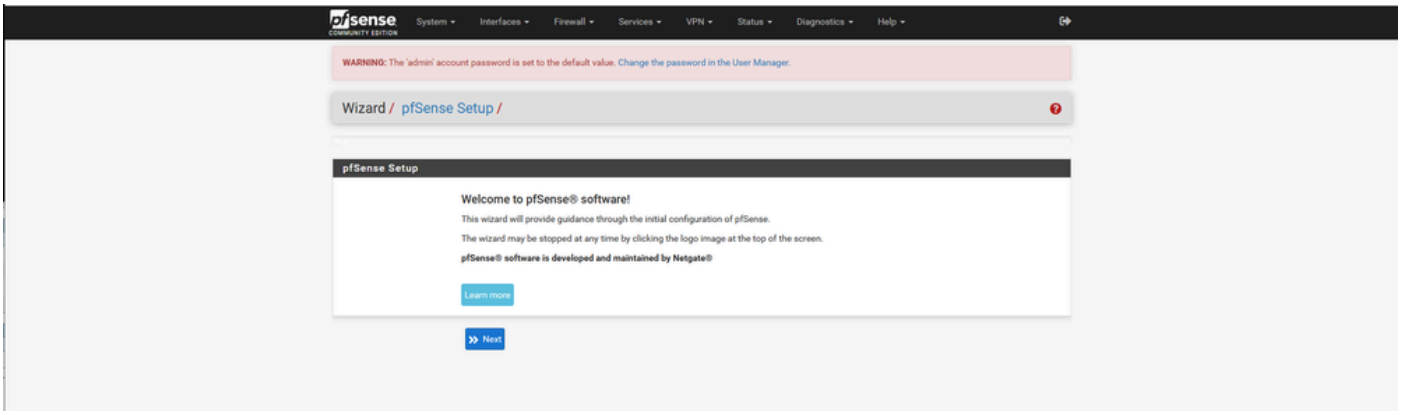


Accesso amministratore pfSense

Passaggio 2. Accedere con il login predefinito di admin / pfSense

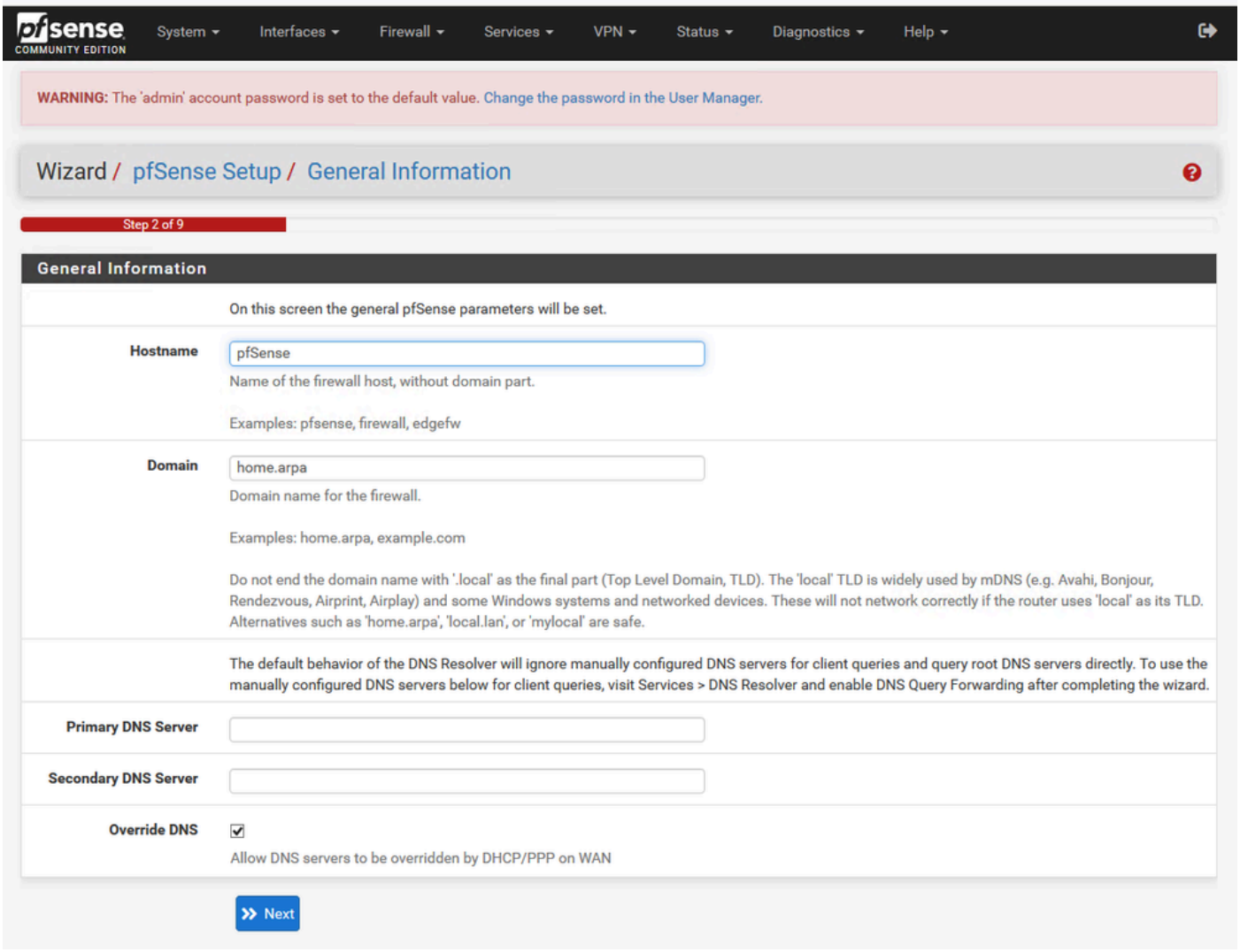
Passaggio 3. Completare la configurazione iniziale

Fare clic su Avanti nelle prime due schermate.



Installazione guidata di pfSense - 1

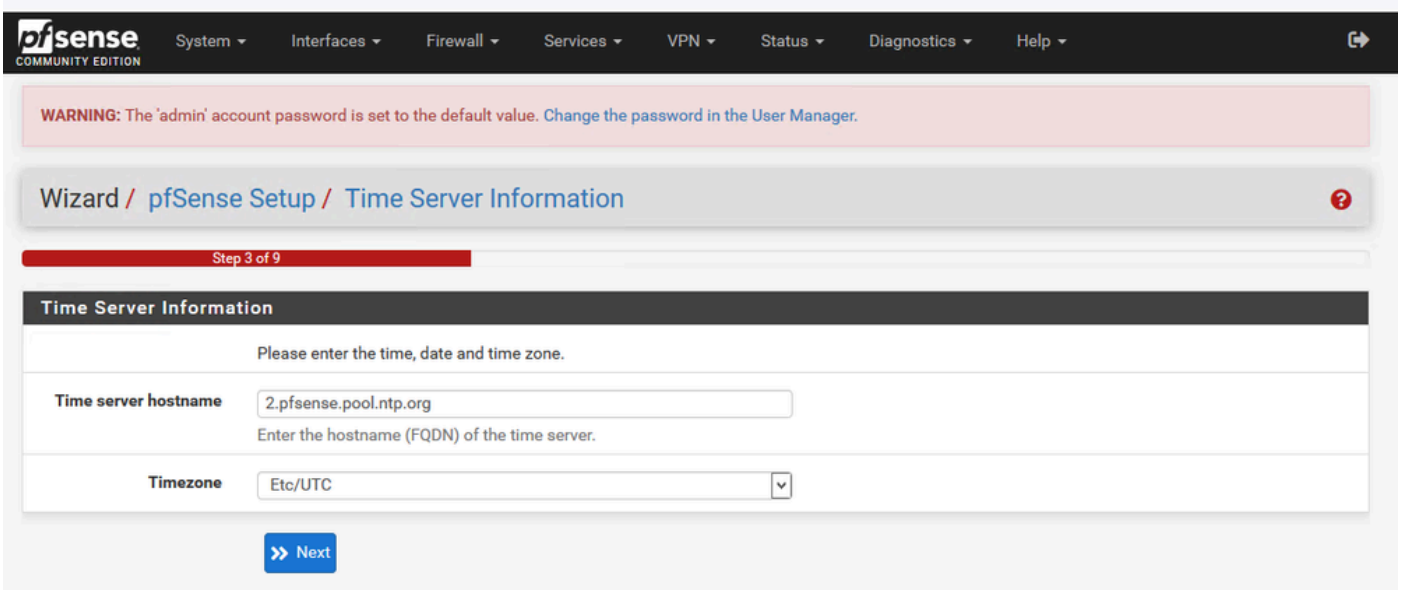
Specificare il nome dell'host, il nome di dominio e le informazioni sul server DNS.



Installazione guidata di pfSense - 2

Convalidare le informazioni sull'indirizzo IP. Se all'inizio è stato scelto DHCP, è possibile modificarlo ora.

Fornire il nome host del Time server NTP e selezionare il fuso orario corretto nell'elenco a discesa.



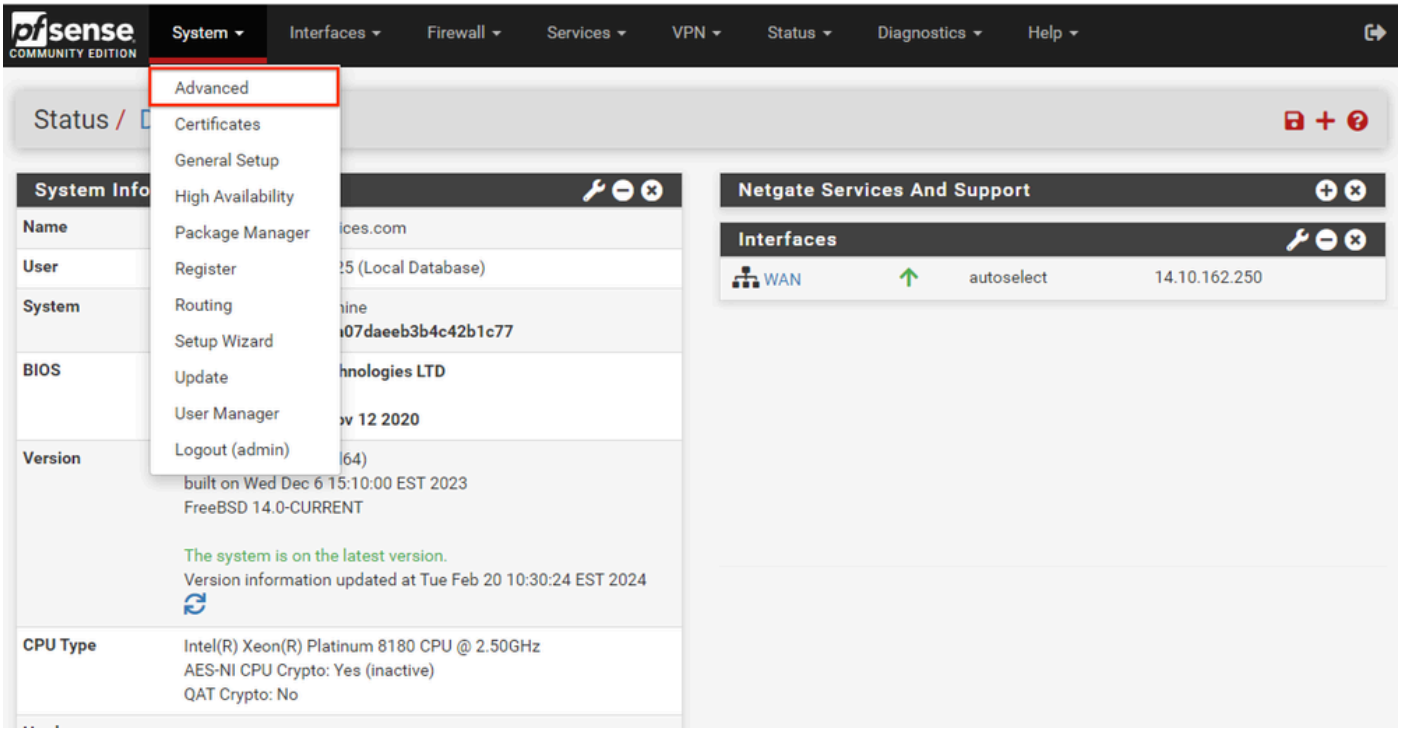
Installazione guidata di pfSense - 3

Continuare l'installazione guidata fino alla fine. La GUI dell'interfaccia si riavvia e l'utente viene reindirizzato al nuovo URL una volta completato.

Configurazione delle impostazioni di amministrazione di base

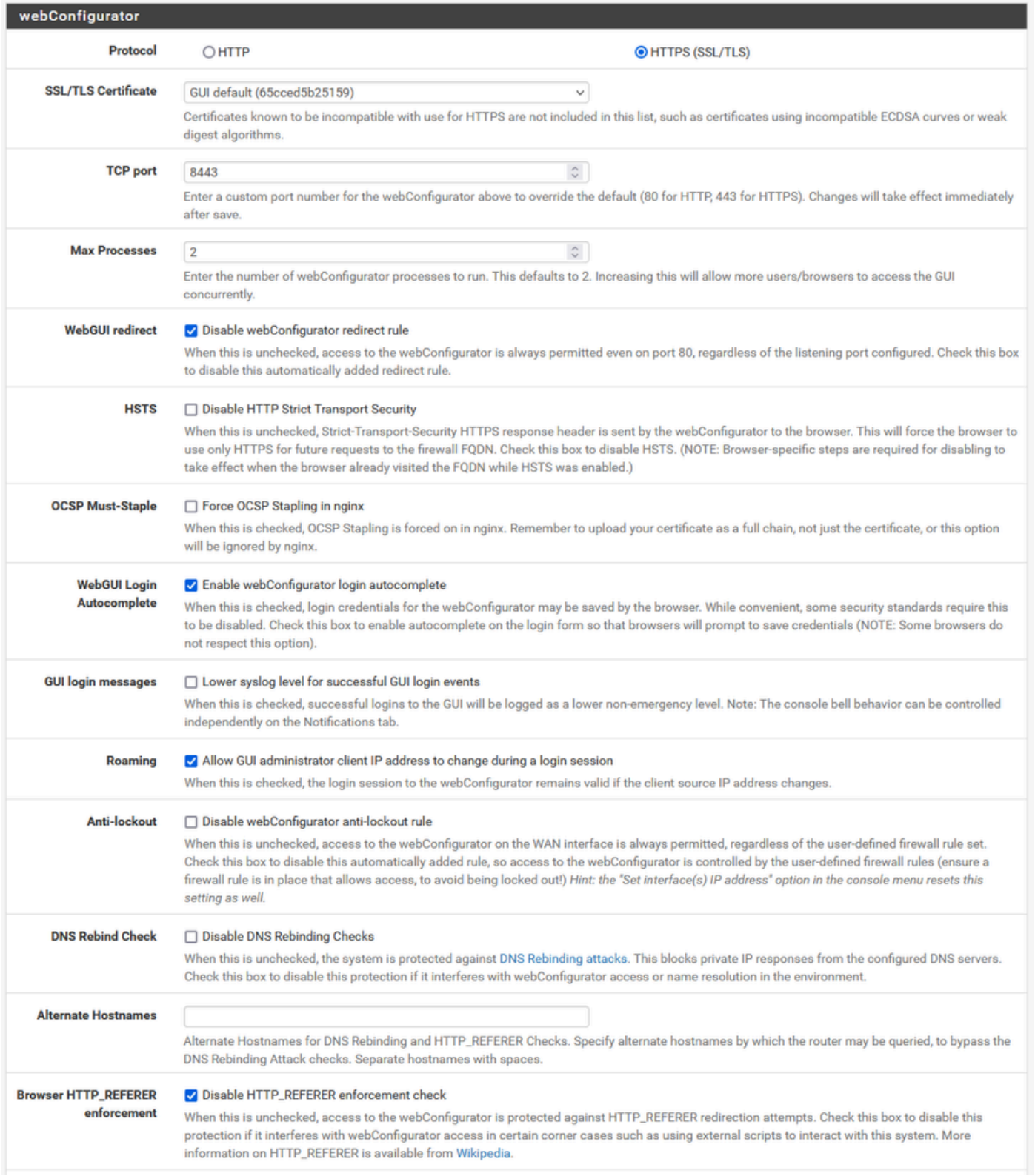
Passaggio 1. Accedere all'interfaccia di amministrazione

Passaggio 2. Selezionare Avanzate dal menu a discesa Sistema.



pfSense GUI - Menu a discesa Amministratore

Passaggio 3. Aggiorna impostazioni WebConfigurator



GUI pfSense - Configurazione amministratore

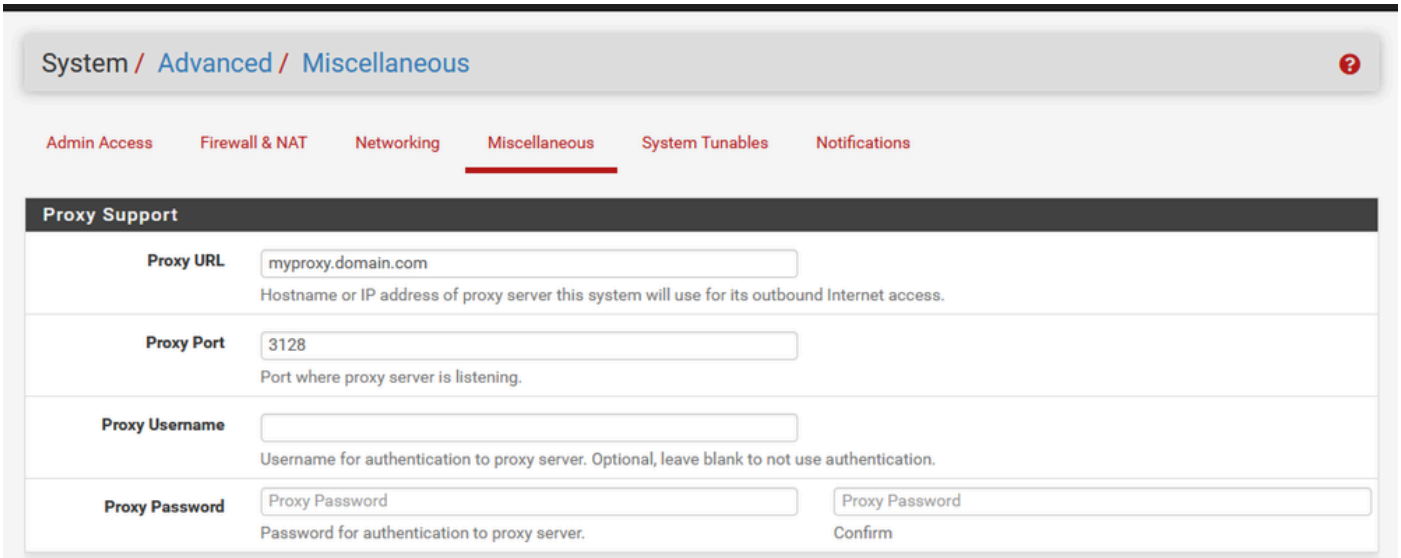
1. Selezionare il protocollo HTTPS (SSL/TLS).
2. In questo momento, lasciare il certificato SSL/TLS sul certificato autofirmato.
3. Modificare la porta TCP su una porta diversa dalla porta 443 per proteggere meglio l'interfaccia e prevenire problemi di sovrapposizione delle porte.
4. Selezionare l'opzione di reindirizzamento WebGUI per disabilitare l'interfaccia di amministrazione sulla porta 80.
5. Selezionare l'opzione di imposizione Browser HTTP_REFERER.

6. Abilitare Secure Shell selezionando l'opzione Abilita Secure Shell.

Nota: selezionare il pulsante Salva prima di procedere. L'utente viene quindi reindirizzato al nuovo collegamento https.

Passaggio 4. Configurare il server proxy, se necessario

Se necessario, configurare le informazioni sul proxy nella scheda Varie. Per completare l'installazione e la configurazione, l'accessorio deve disporre di accesso a Internet.



pfSense GUI - Configurazione proxy

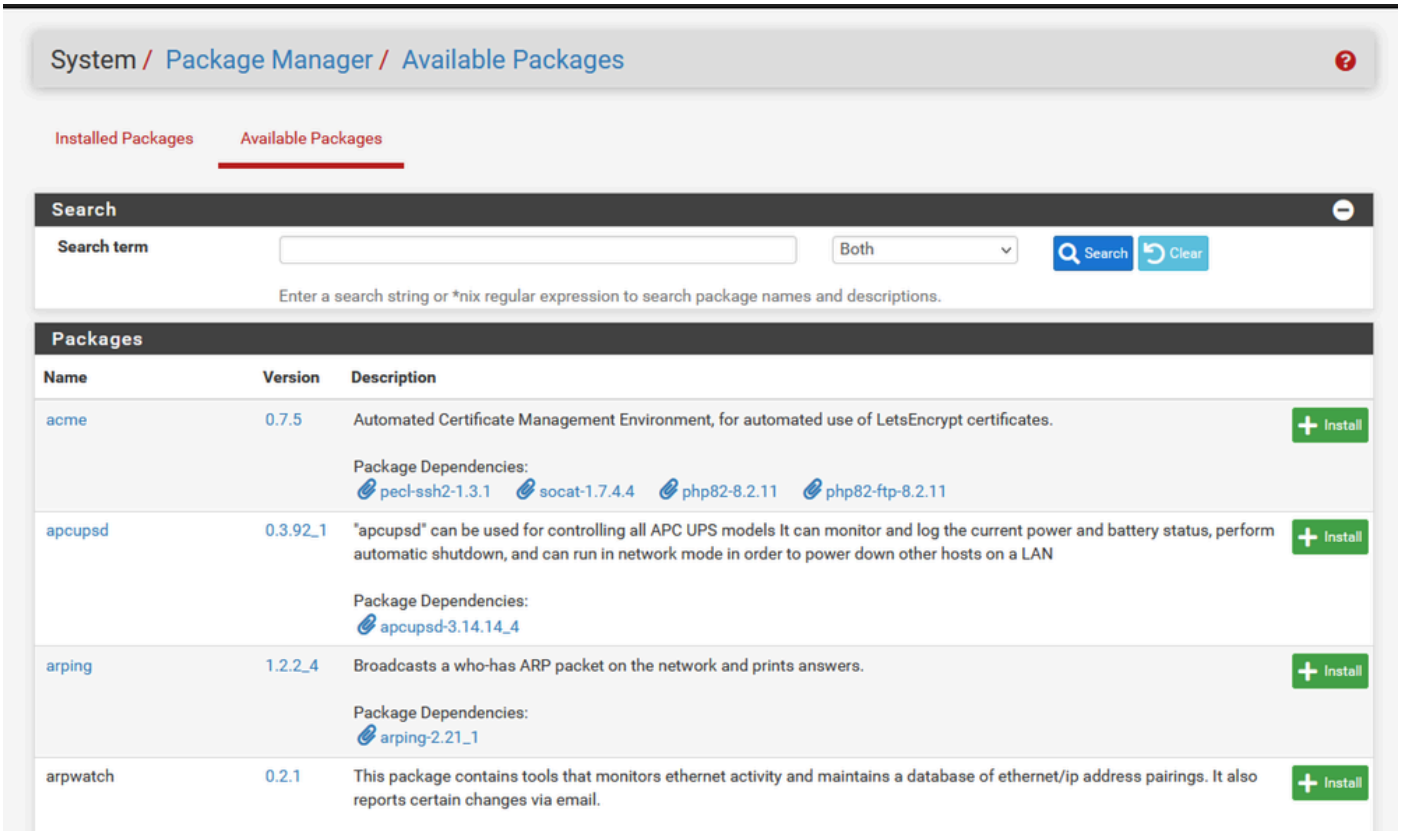
Nota: assicurarsi di selezionare il pulsante Salva dopo aver apportato le modifiche.

Aggiungi pacchetti richiesti

Passaggio 1. Selezionare Sistema > Gestione pacchetti

Passaggio 2. Seleziona pacchetti disponibili

Nota: il caricamento di tutti i pacchetti disponibili può richiedere alcuni minuti. Se si verifica il timeout, verificare che i server DNS siano configurati correttamente. Spesso il riavvio dell'accessorio risolve il problema della connettività Internet.



pfSense GUI - Elenco pacchetti

Passaggio 3. Trova e installa i pacchetti richiesti

1. haproxy
2. Open-VM-Tools

Nota: non selezionare il pacchetto haproxy-devel.

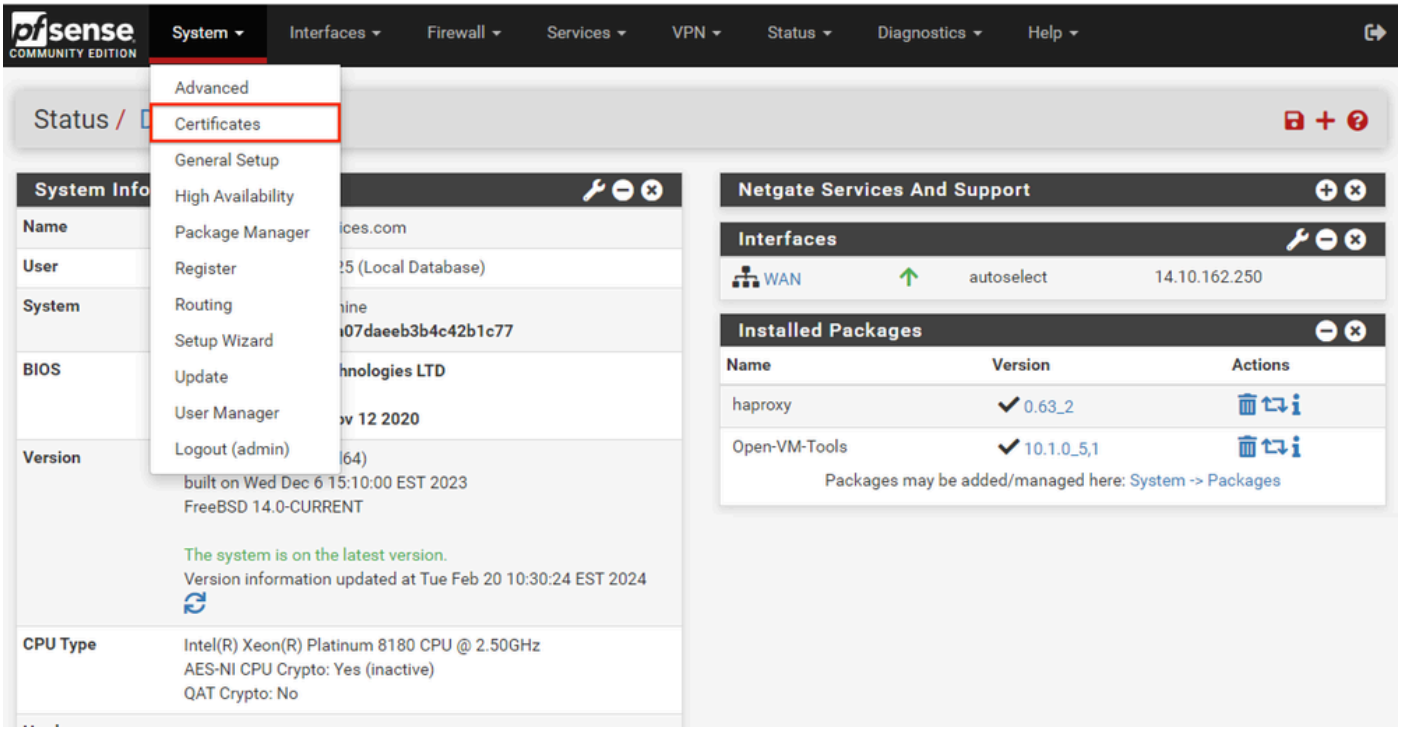
Configura certificati

pfSense può creare un certificato autofirmato o integrarsi con una CA pubblica, una CA interna, oppure può fungere da CA e rilasciare certificati firmati dalla CA. In questa guida vengono illustrati i passaggi da integrare con una CA interna.

Prima di iniziare questa sezione, assicurarsi di avere a disposizione questi elementi.

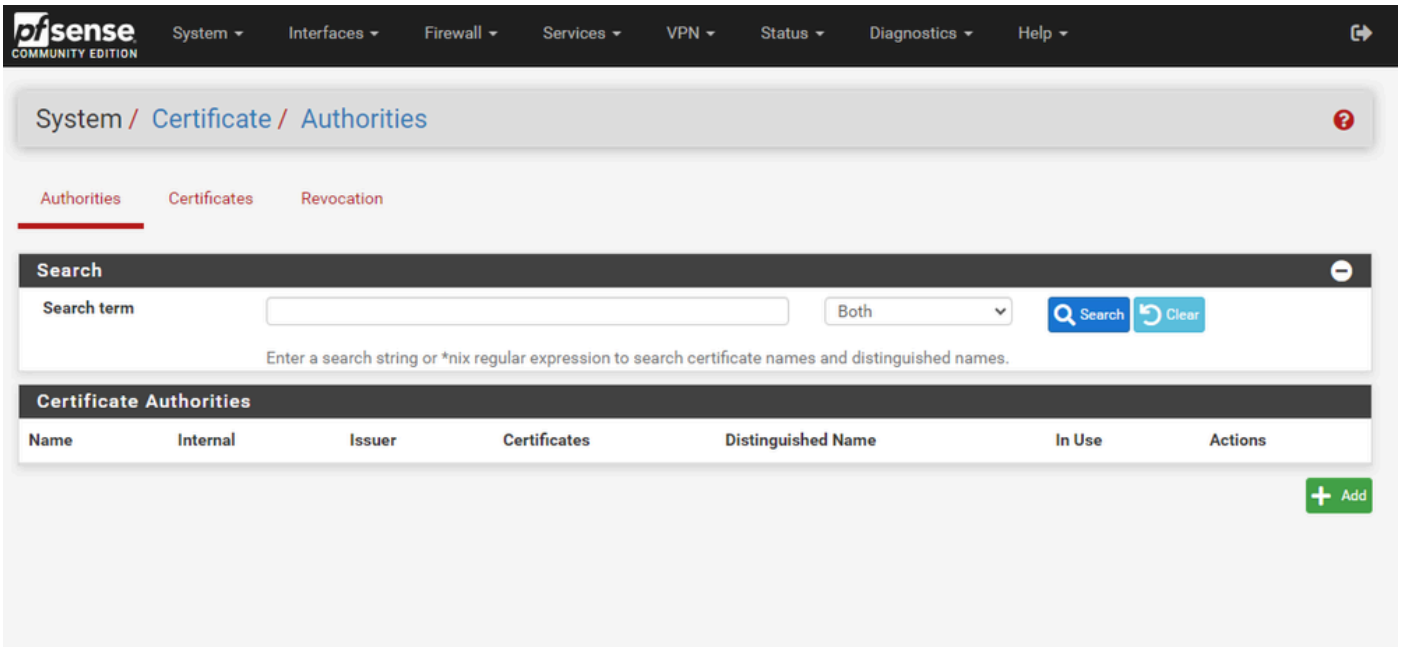
1. Certificato radice per CA salvato in formato PEM o con codifica Base 64.
2. Tutti i certificati intermedi (talvolta denominati emettere) per CA salvati come formato PEM o con codifica Base 64.

Passaggio 1. Selezionare Certificati dal menu a discesa Sistema.



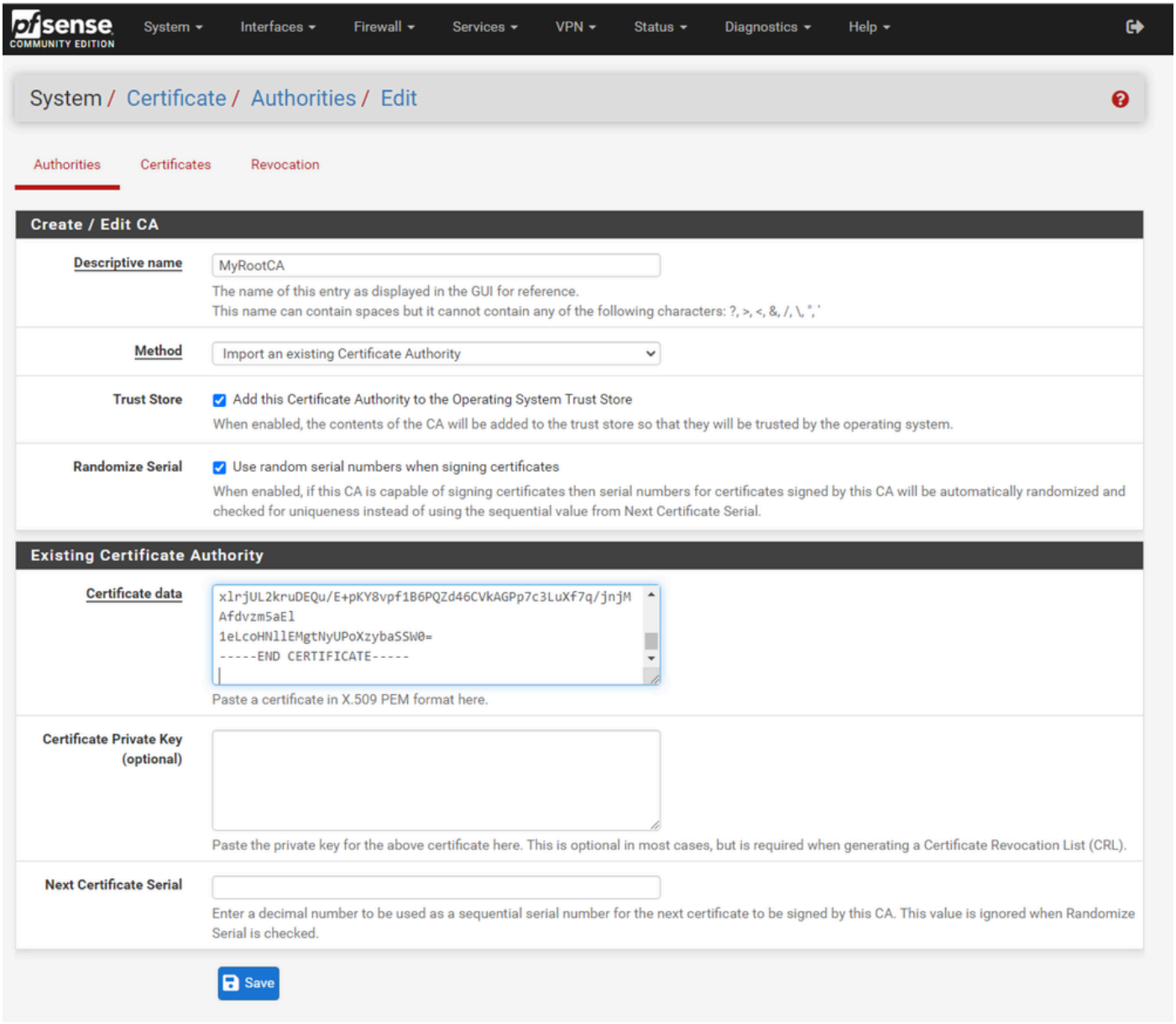
pfSense GUI - Elenco a discesa dei certificati

Passaggio 2. Importa certificato radice CA



pfSense GUI - Elenco certificati CA

Selezionare il pulsante Aggiungi.



PfSense GUI - Importazione CA

Come mostrato nell'immagine:

1. Fornire un nome univoco e descrittivo

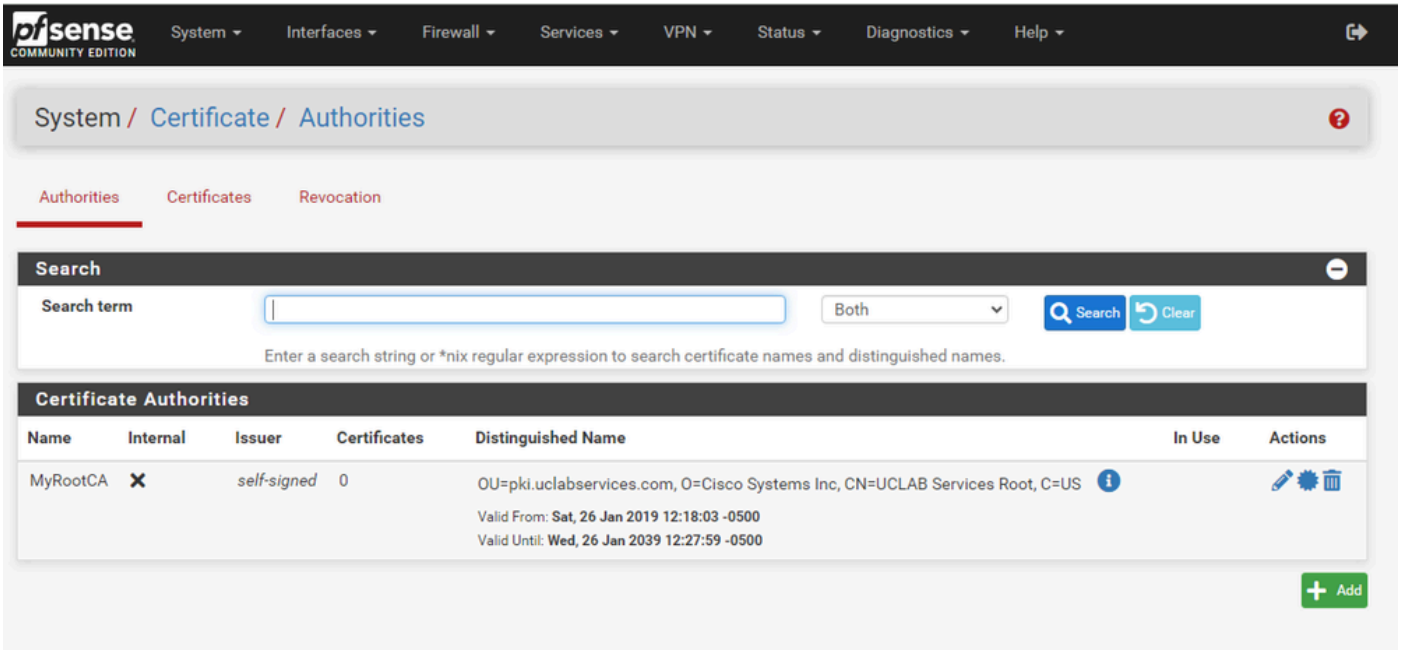
2. Selezionare Importa un'autorità di certificazione esistente dall'elenco a discesa Metodo.

3. Verificare che le caselle di controllo Archivio attendibile e Numero di serie casuale siano selezionate.

4. Incollare l'intero certificato nella casella di testo Dati certificato. Assicurarsi di includere dalle righe —BEGIN CERTIFICATE— e —END CERTIFICATE—.

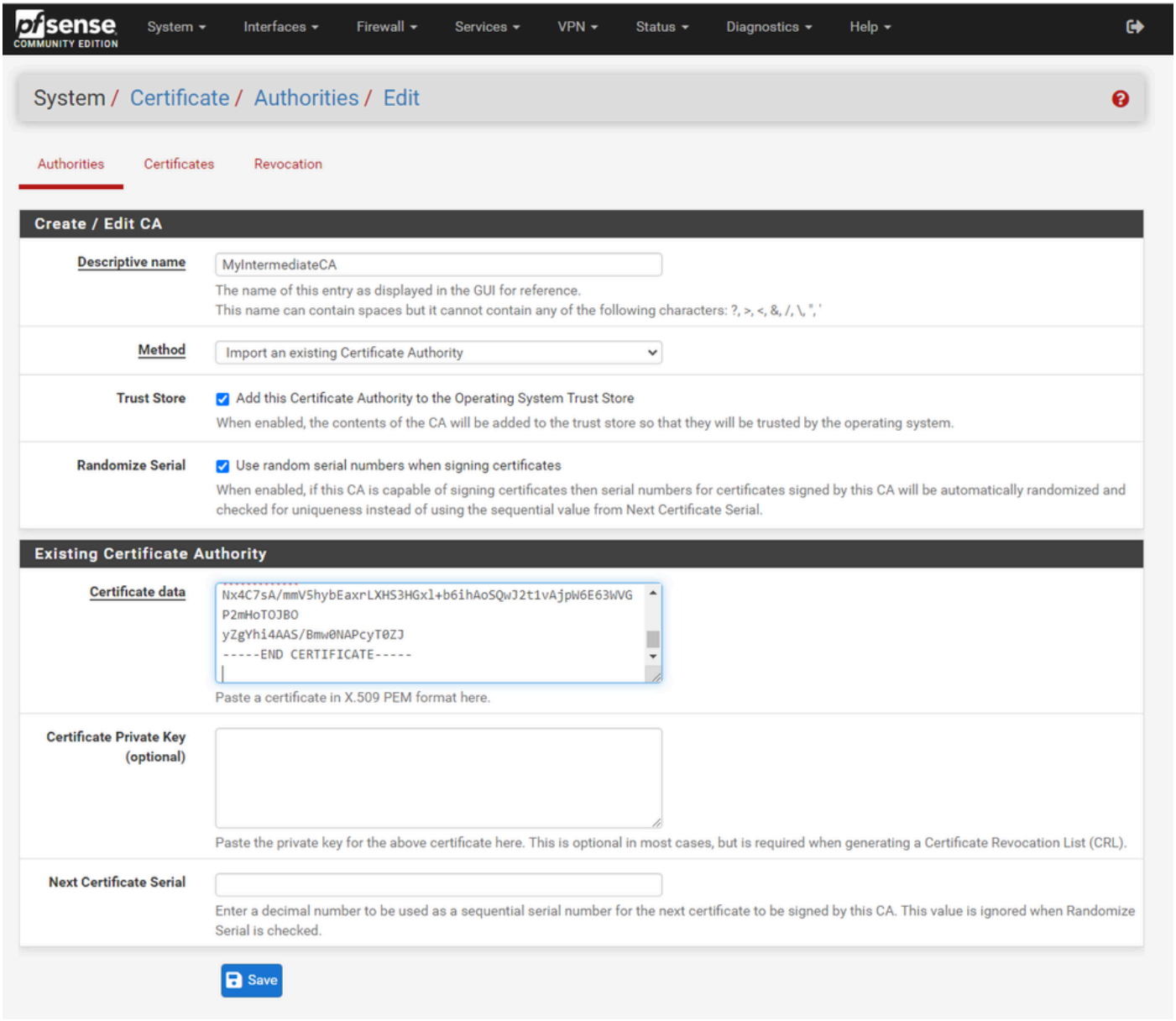
5. Selezionare Salva.

6. Verificare che il certificato sia stato importato come mostrato nell'immagine.



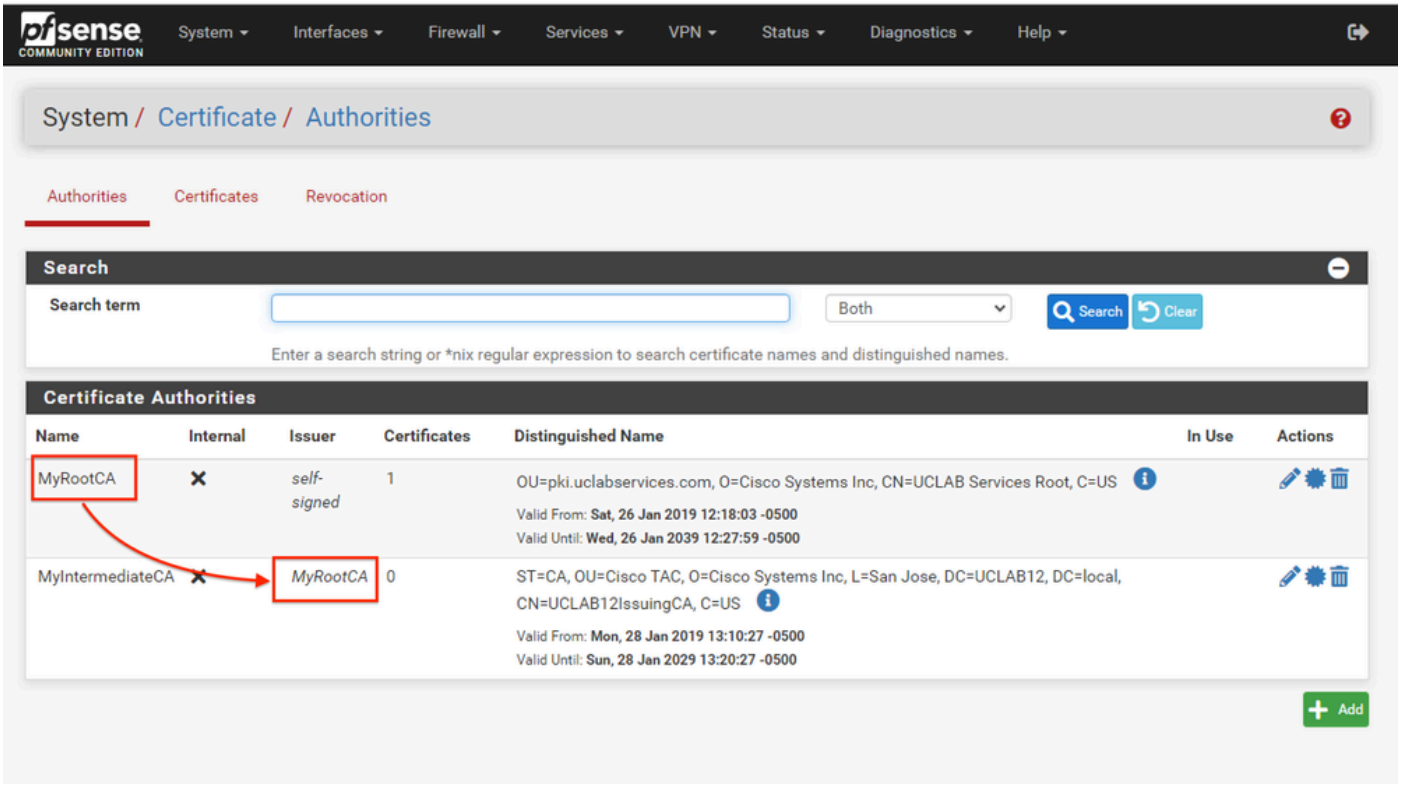
pfSense GUI - Elenco CA

Passaggio 3. Importa certificato intermedio CA



PfSense GUI - Importazione intermedia CA

Ripetere i passaggi per importare il certificato CA radice per importare il certificato CA intermedio.



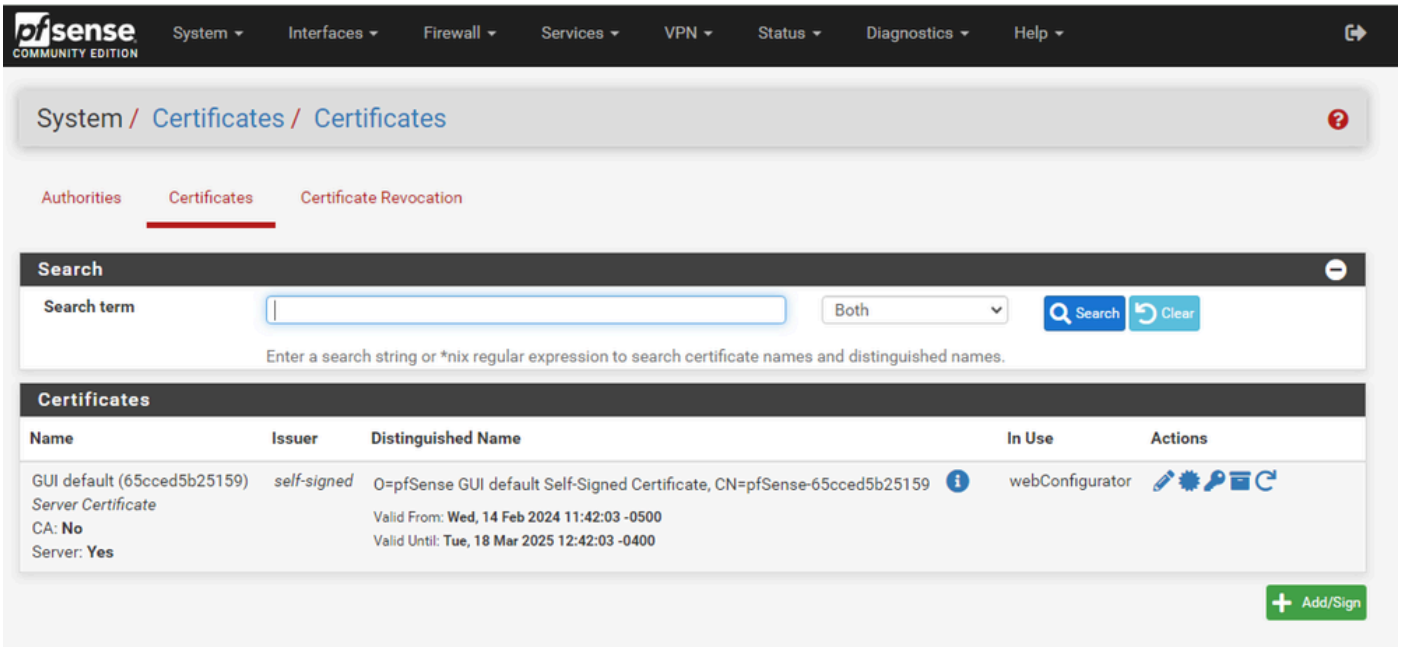
Interfaccia utente di pfSense - Collegamenti CA

Esaminare le Autorità di certificazione per verificare che il certificato intermedio sia correttamente concatenato al certificato radice, come mostrato nell'immagine.

Passaggio 4. Creare ed esportare un CSR per il sito Web con carico bilanciato

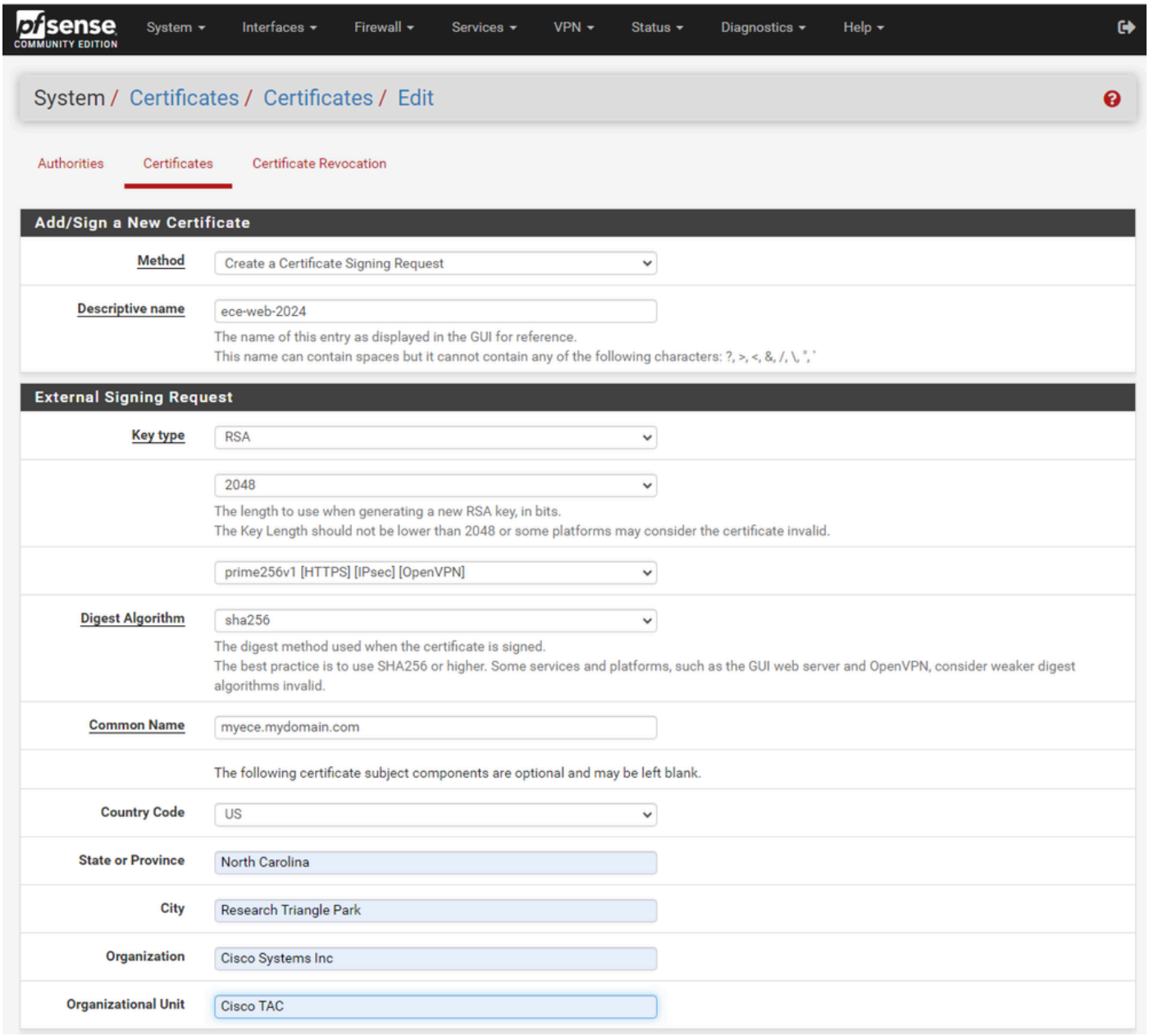
In questa sezione vengono descritti i passaggi necessari per creare un CSR, esportare il CSR e quindi importare il certificato firmato. Se si dispone già di un certificato in formato PFX, è possibile importare questo certificato. Consultare la documentazione di pfSense per questi passaggi.

1. Selezionare il menu Certificati, quindi selezionare il pulsante Aggiungi/Firma.



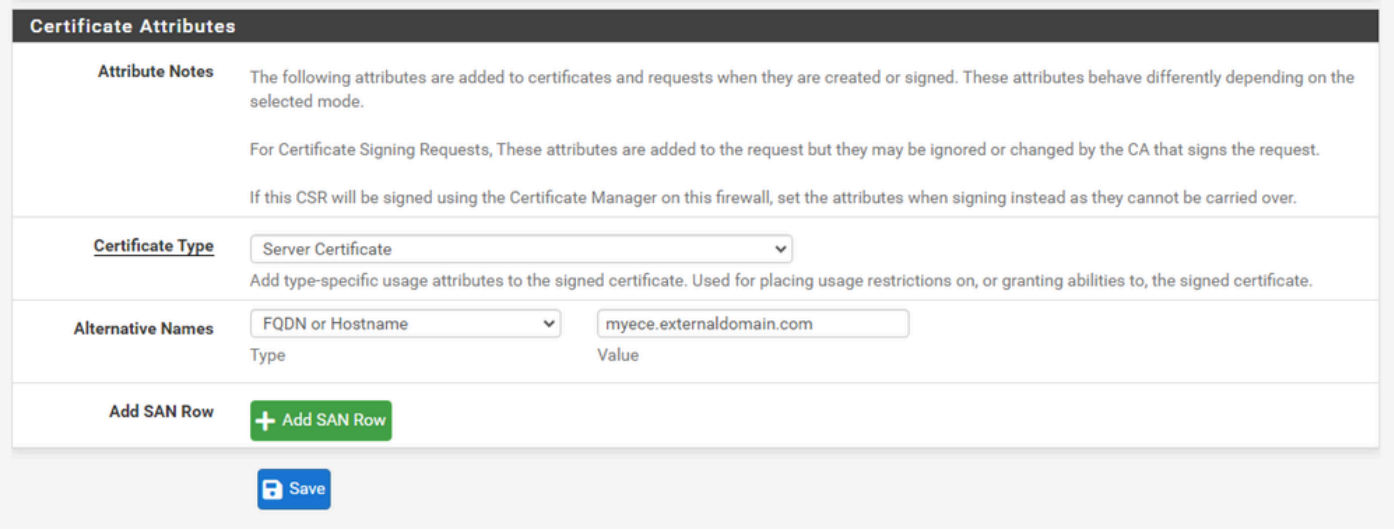
pfSense GUI - Elenco certificati

2. Completare il modulo di richiesta di firma del certificato.



GUI pfSense - Creazione CSR

- Metodo: selezionare Crea richiesta di firma certificato dall'elenco a discesa.
- Nome descrittivo: fornire un nome per il certificato
- Tipo di chiave e algoritmo digest: rivedere per verificare che soddisfino i requisiti
- Nome comune: fornire il sito Web del nome di dominio completo
- Fornire le restanti informazioni sul certificato necessarie per l'ambiente in uso



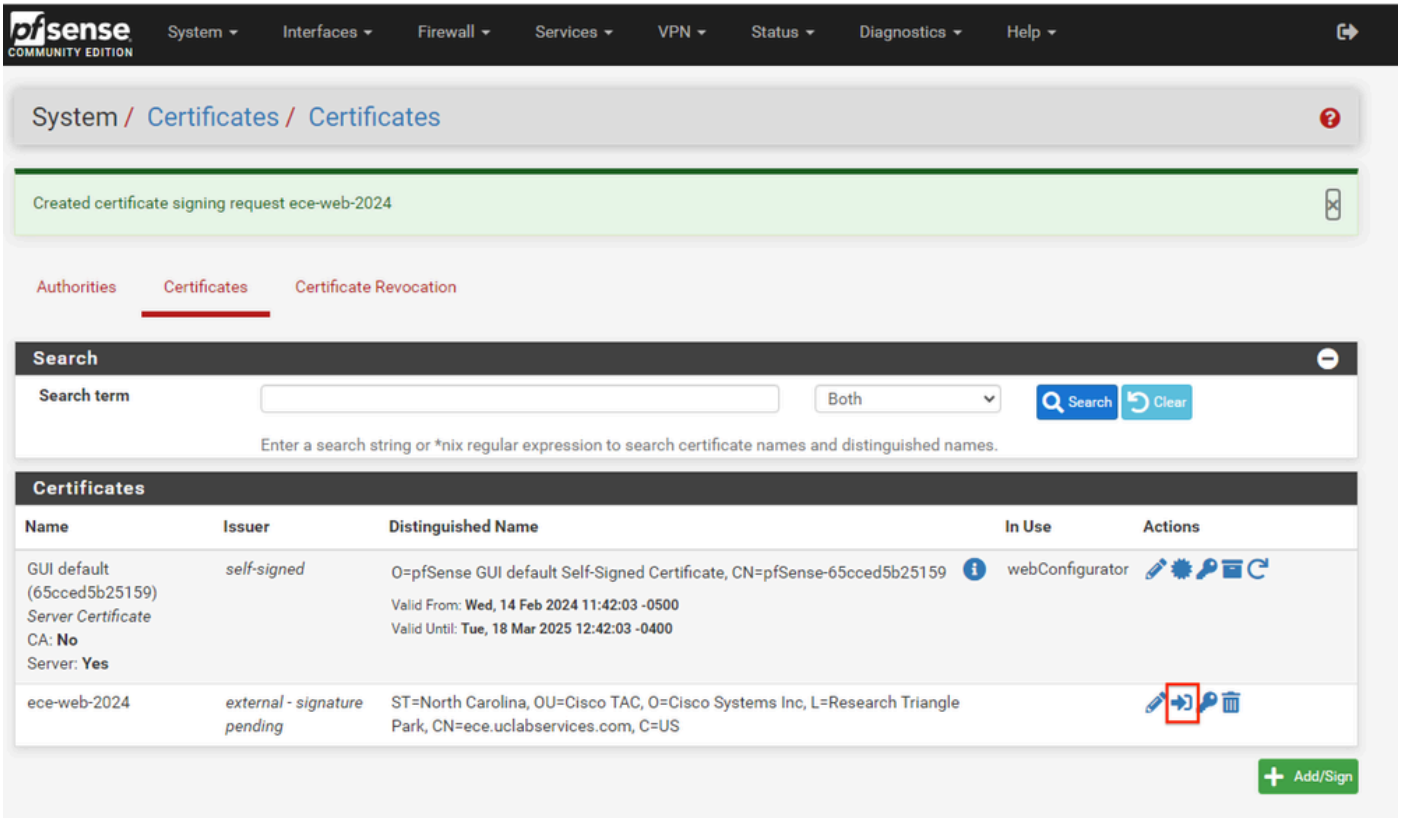
GUI pfSense - CSR avanzata

- Tipo di certificato: selezionare Certificato server nell'elenco a discesa.
- Nomi alternativi: fornire tutti i nomi alternativi soggetto (SAN) necessari per l'implementazione.

Nota: il nome comune viene aggiunto automaticamente al campo SAN. È sufficiente aggiungere altri nomi.

Selezionare Salva una volta che tutti i campi sono corretti.

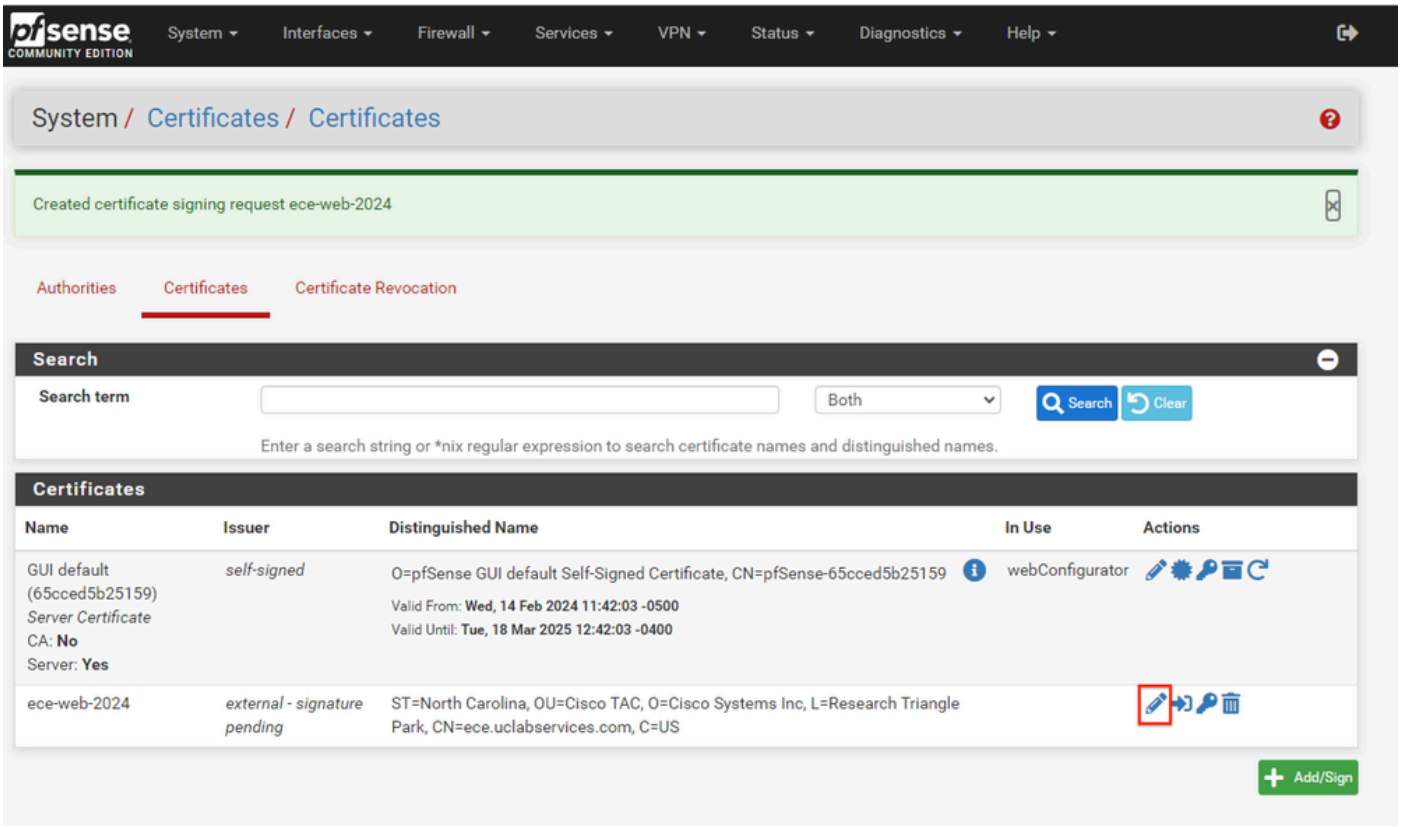
3. Esportare il file CSR in un file.



GUI pfSense - Esportazione CSR

Selezionare il pulsante Esporta per salvare il CSR, quindi firmarlo con la CA. Una volta ottenuto il certificato firmato, salvarlo come file PEM o Base-64 per completare il processo.

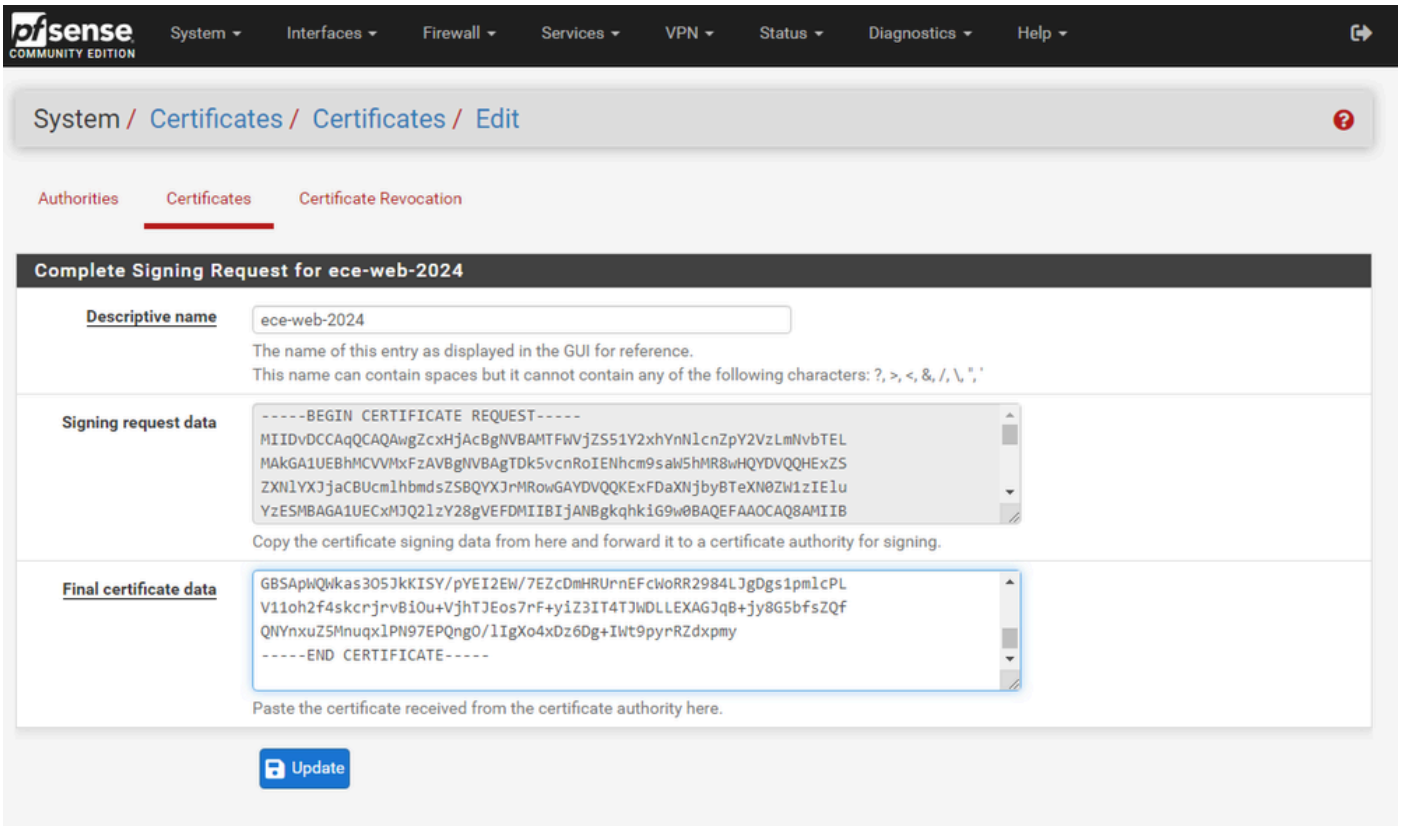
4. Importare il certificato firmato.



pfSense GUI - Importazione certificati

Selezionare l'icona Matita per importare il certificato firmato.

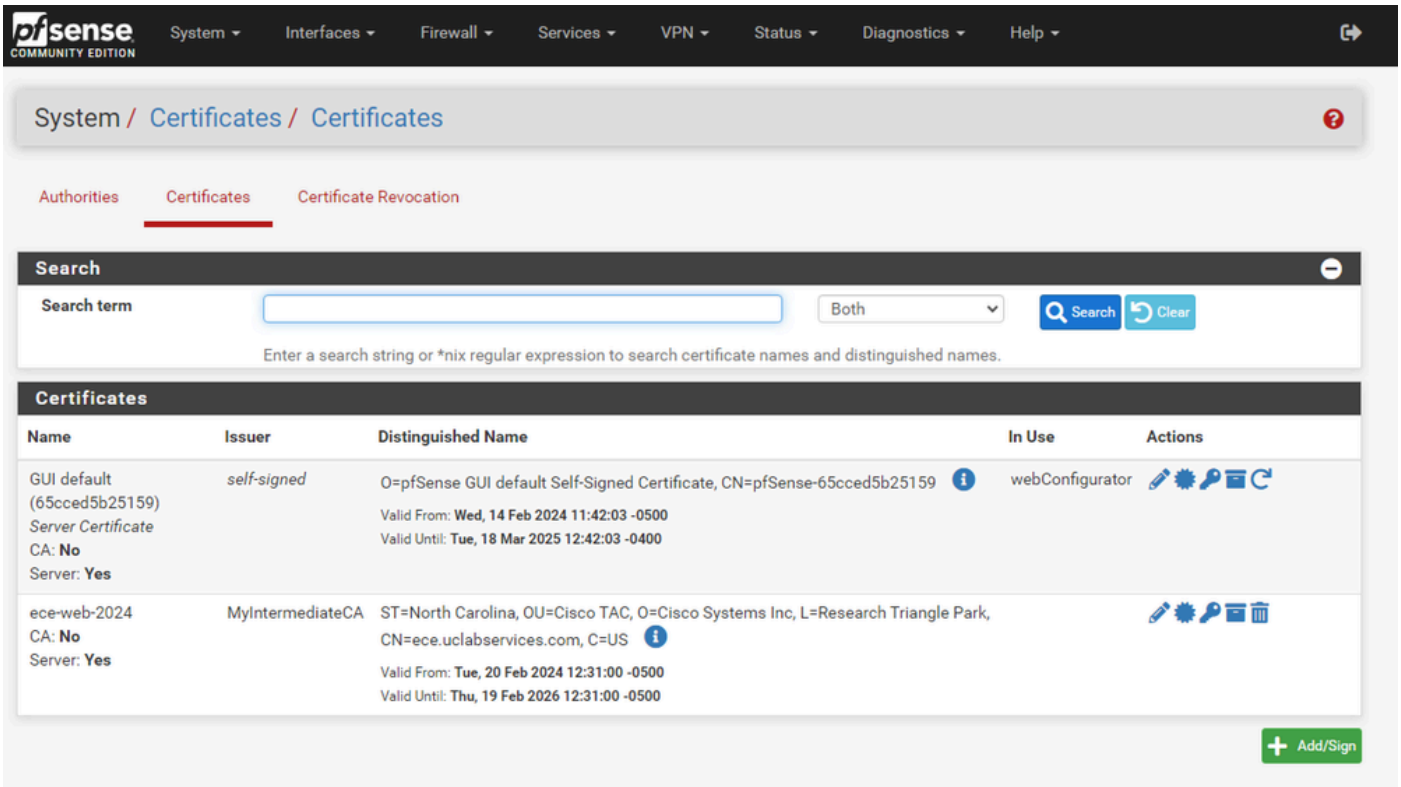
5. Incollare i dati del certificato nel modulo.



pfSense GUI - Importazione certificati

Selezionare Aggiorna per salvare il certificato.

6. Esaminare i dati del certificato per accertarsi che siano corretti.



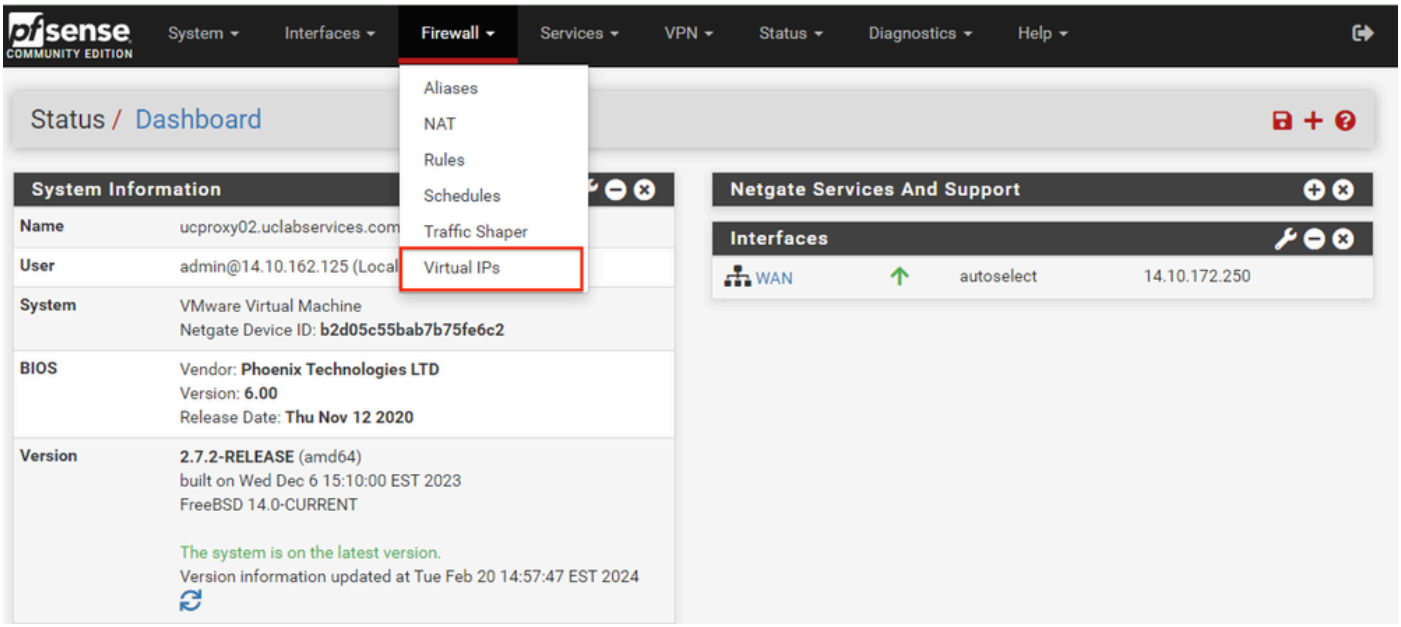
pfSense GUI - Elenco certificati

7. Ripetere questa procedura se si desidera ospitare più siti su questo pfSense.

Aggiungi IP virtuali

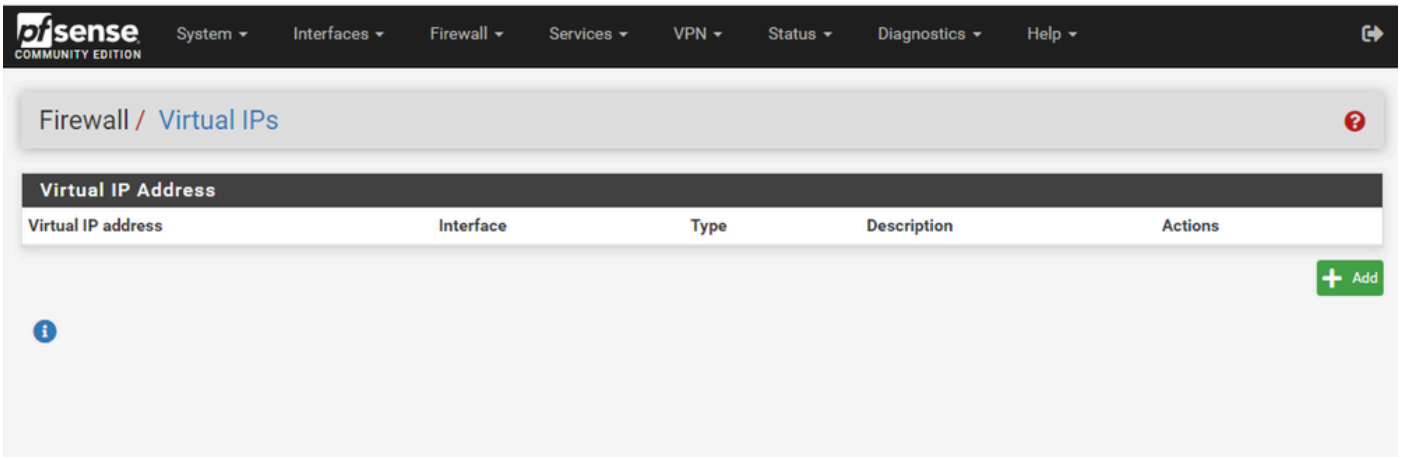
È necessario almeno un indirizzo IP per ospitare i siti Web in pfSense. In pfSense ciò viene fatto con gli IP virtuali (VIP).

Passaggio 1. Selezionare IP virtuali dall'elenco a discesa Firewall



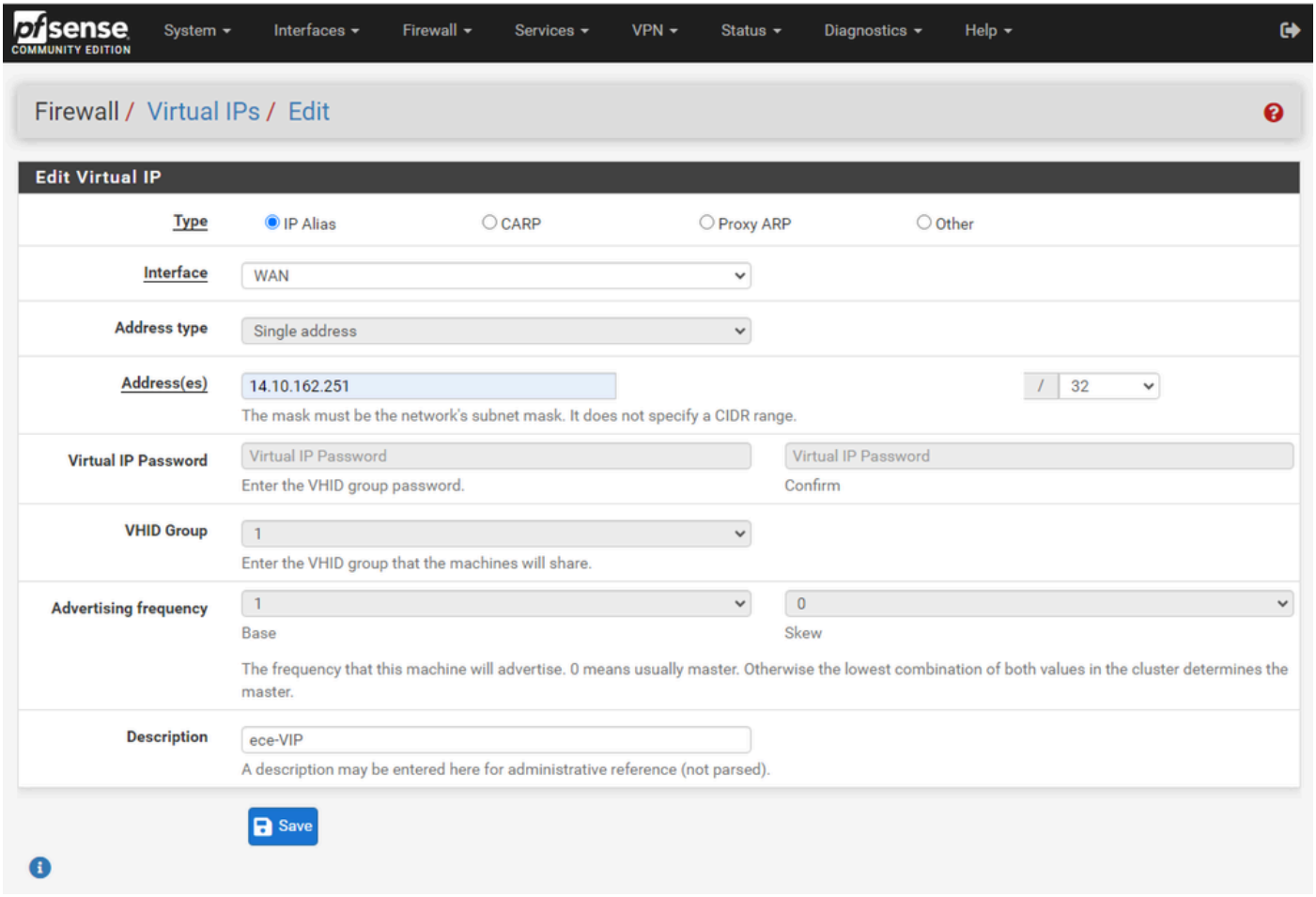
GUI pfSense - Elenco a discesa VIP

Passaggio 2. Selezionare il pulsante Aggiungi



GUI pfSense - Pagina iniziale VIP

Passaggio 3. Fornire informazioni sull'indirizzo



GUI pfSense - Configurazione VIP

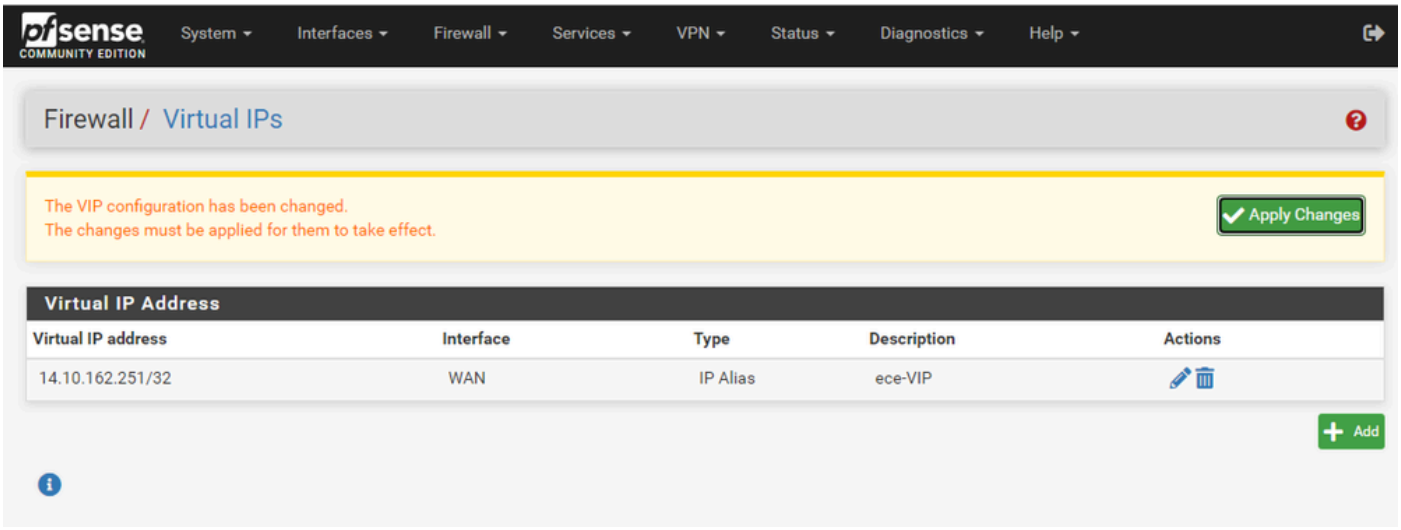
Utilizzare le informazioni per aggiungere un VIP.

- Tipo: Seleziona alias IP
- Interfaccia: selezionare l'interfaccia per l'indirizzo IP da trasmettere
- Indirizzi: immettere l'indirizzo IP
- Maschera indirizzo: per gli indirizzi IP utilizzati per il bilanciamento del carico, la maschera deve essere una /32
- Descrizione: fornire un breve testo per semplificare la comprensione della configurazione in un secondo momento

Selezionare Salva per eseguire il commit della modifica.

Ripetere questa operazione per ciascun indirizzo IP richiesto per la configurazione.

Passaggio 4. Applica configurazione



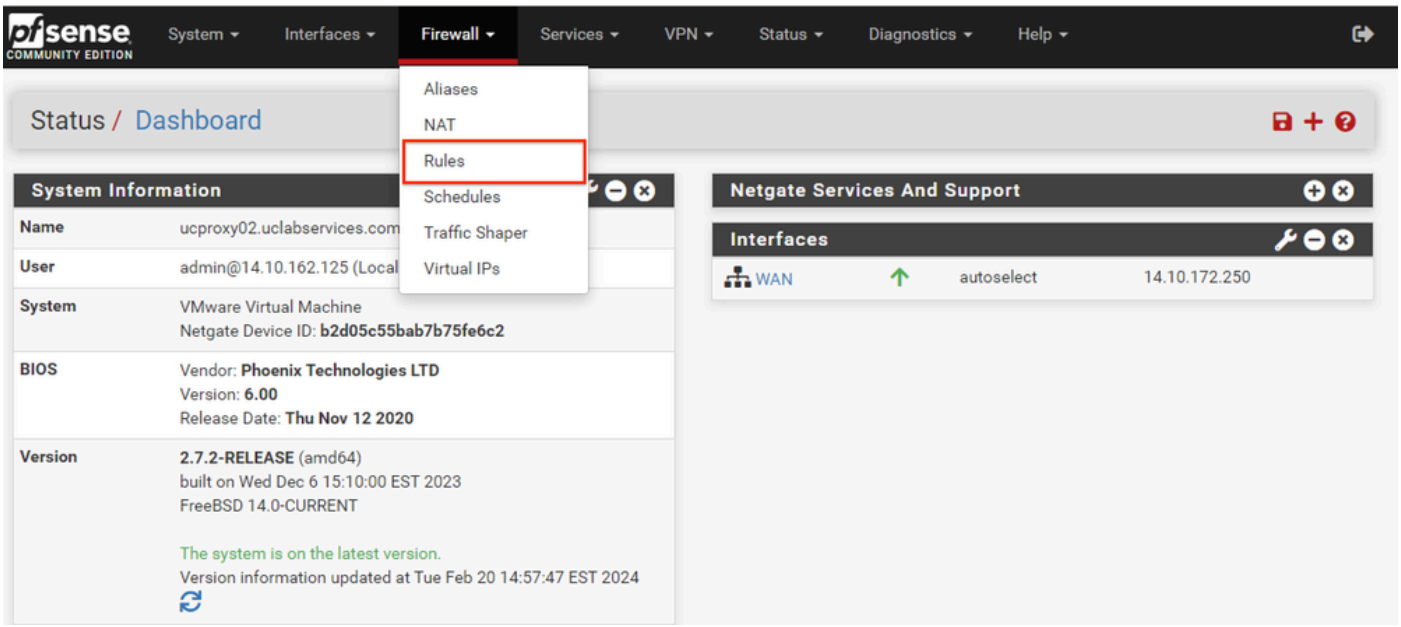
GUI pfSense - Elenco VIP

Selezionare il pulsante Applica modifiche dopo aver aggiunto tutti i VIP.

Configurare il firewall

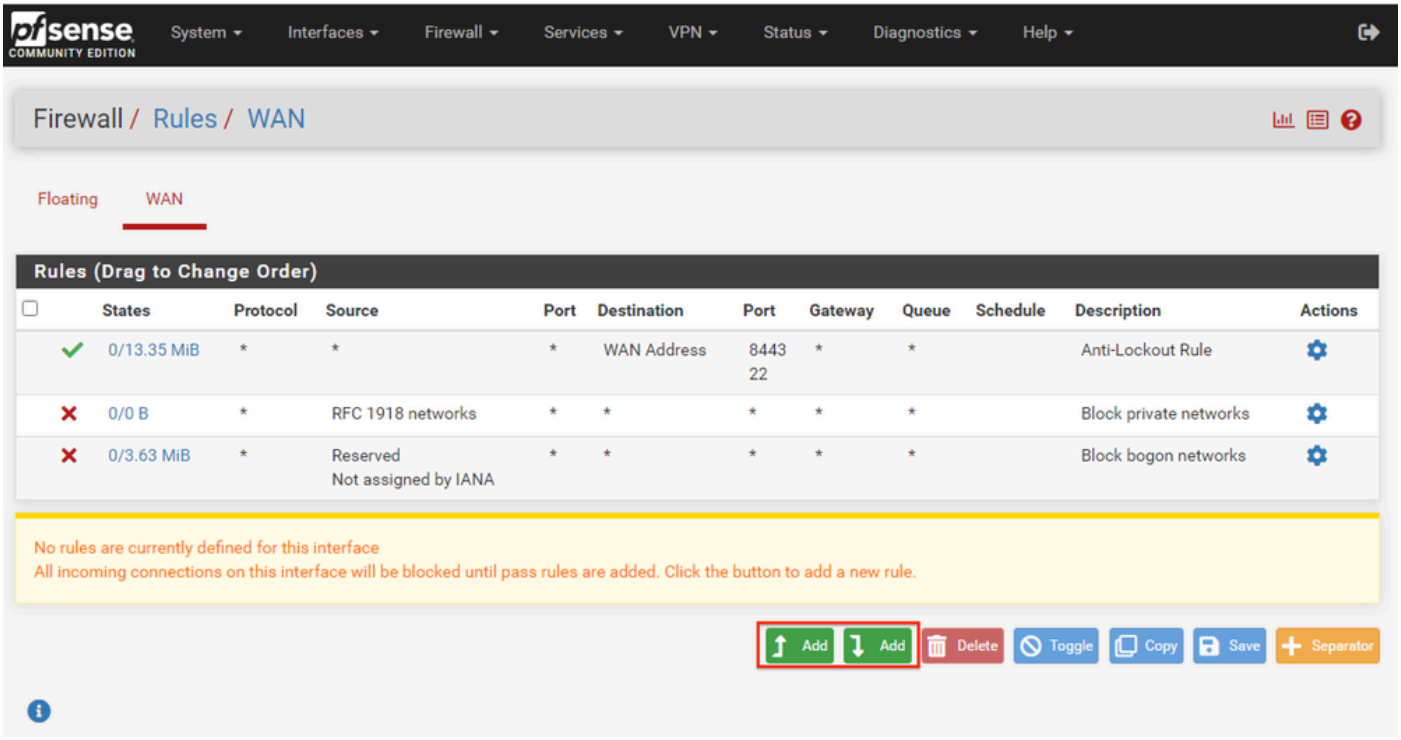
pfSense dispone di un firewall incorporato. Il set di regole predefinito è molto limitato. Prima che l'accessorio venga messo in produzione, è necessario creare una policy firewall completa.

Passaggio 1. Selezionare Regole dall'elenco a discesa Firewall



pfSense GUI - Elenco a discesa delle regole del firewall

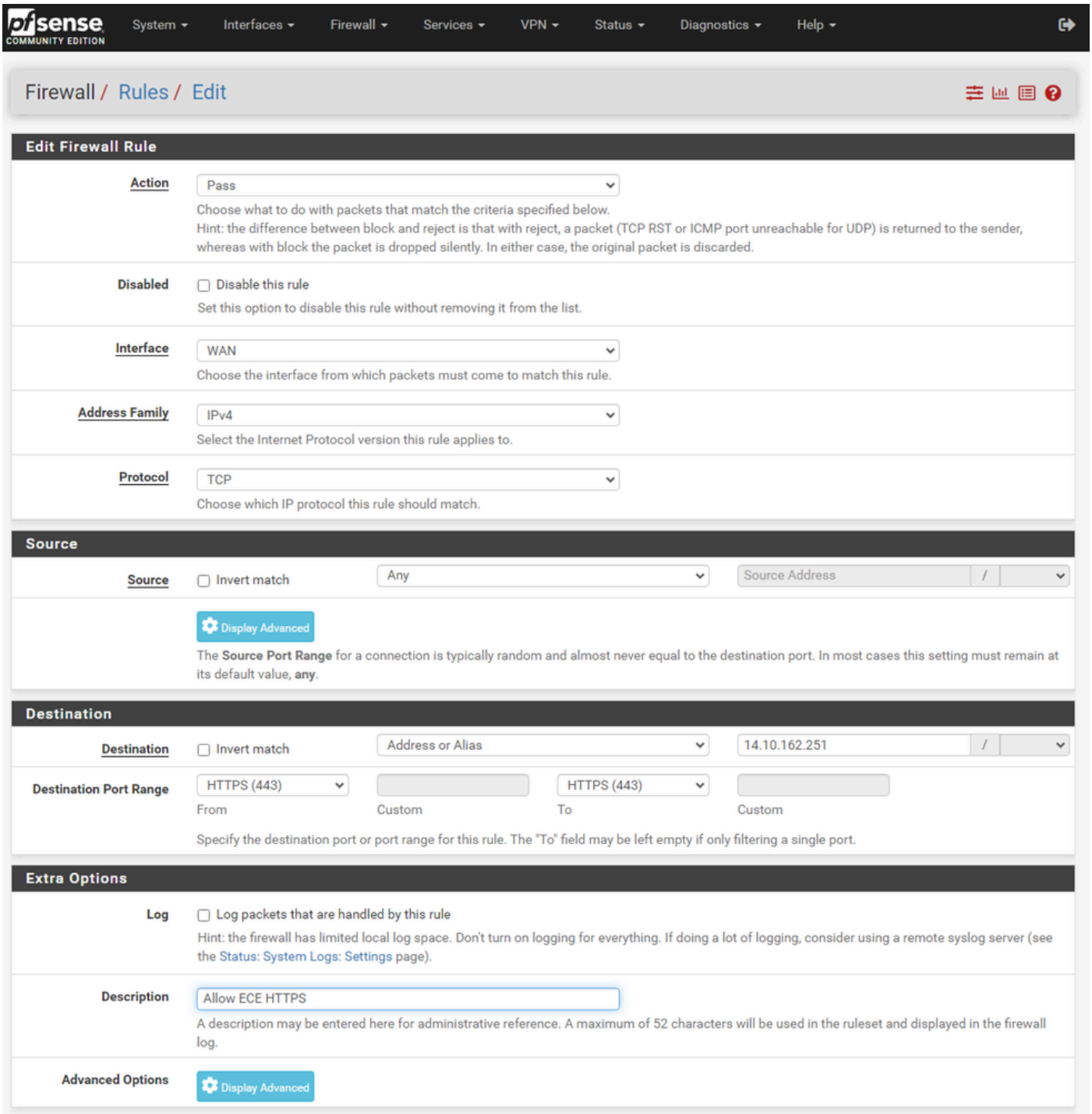
Passaggio 2. Selezionare uno dei pulsanti Aggiungi



pfSense GUI - Elenco regole firewall

Si noti che un pulsante consente di aggiungere la nuova regola sopra la riga selezionata, mentre l'altro consente di aggiungere la regola sotto la regola selezionata. Entrambi i pulsanti possono essere utilizzati per la prima regola.

Passaggio 3. Crea regola firewall per consentire il traffico sulla porta 443 per l'indirizzo IP



GUI pfSense - Configurazione regola passaggio firewall

Utilizzare le informazioni per creare la regola.

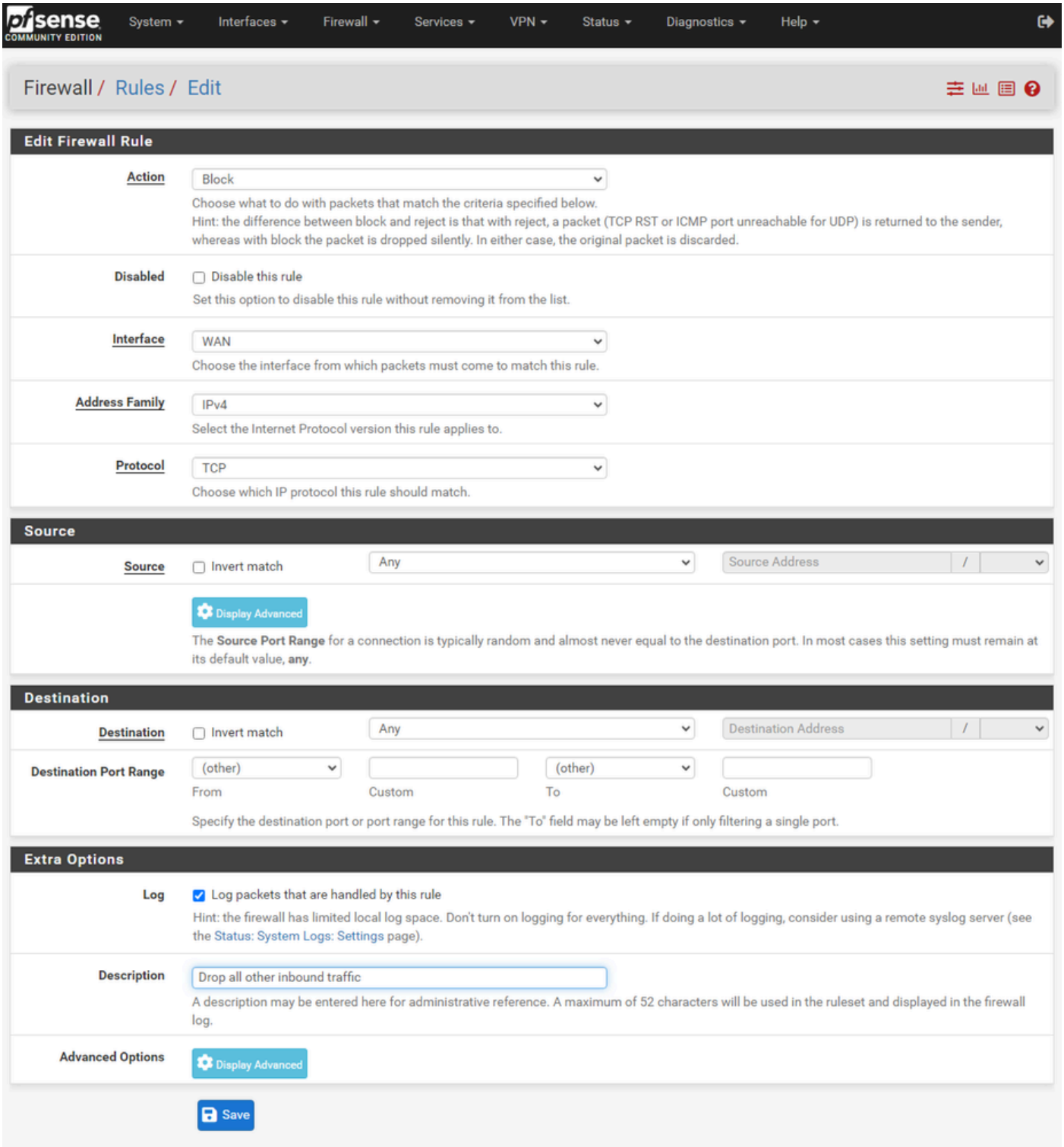
- Azione: Seleziona superamento
- Interfaccia: scegliere l'interfaccia a cui si applica la regola
- Famiglia di indirizzi e protocollo: selezionare la voce appropriata
- Origine: lasciare selezionata l'opzione Qualsiasi
- Destinazione: selezionare Indirizzo o Alias dall'elenco a discesa Destinazione, quindi immettere l'indirizzo IP a cui si applica la regola.
- Intervallo porte di destinazione: selezionare, HTTPS (443) nell'elenco a discesa Da e A
- Registra: selezionare la casella di controllo per registrare tutti i pacchetti che soddisfano questa regola per l'accounting

- Descrizione: fornire il testo per fare riferimento alla regola in seguito

Selezionare Salva.

Passaggio 4. Crea una regola firewall per indirizzare tutto il resto del traffico a pfSense

Selezionare il pulsante Aggiungi per inserire la regola sotto quella appena creata.



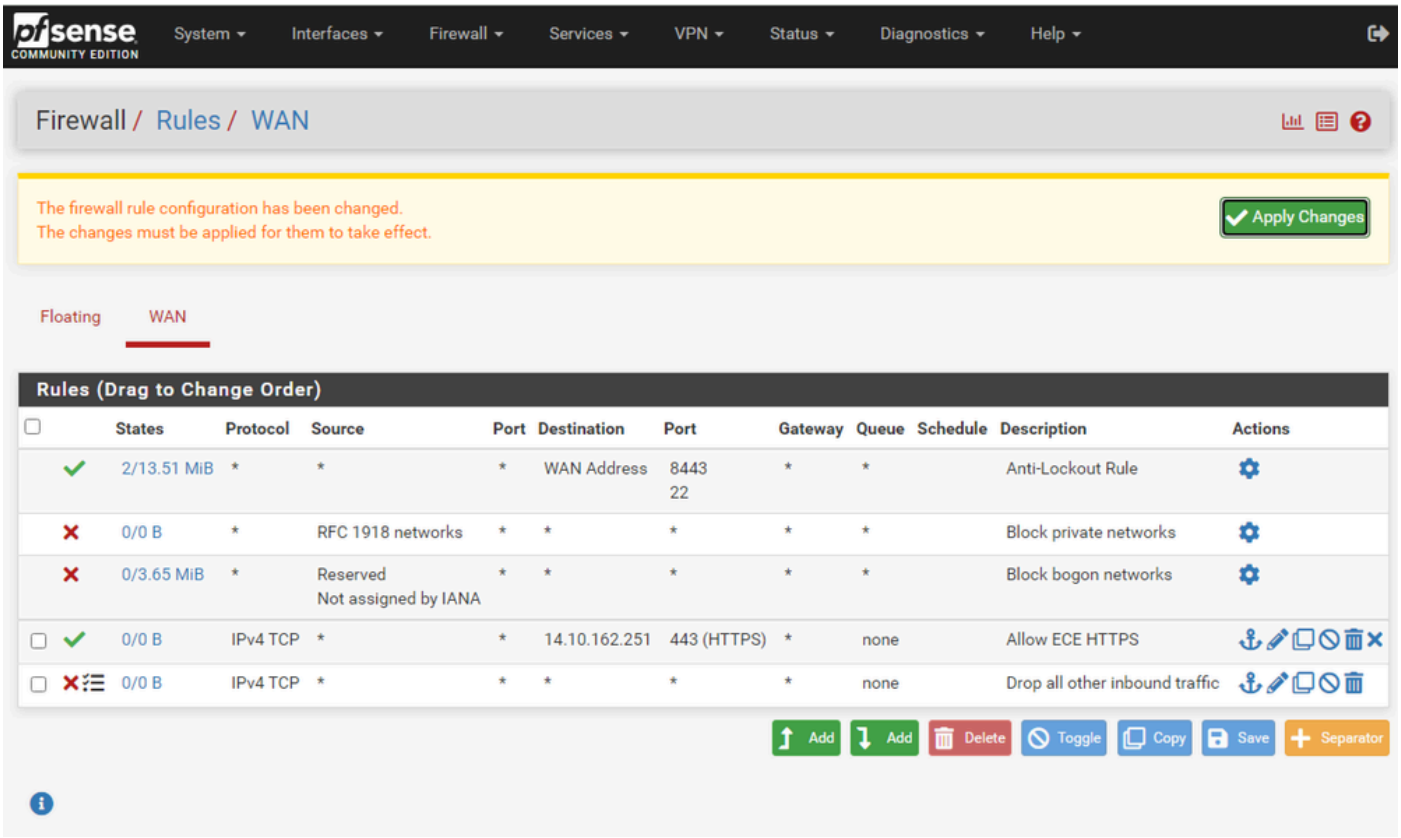
GUI pfSense - Configurazione regola di eliminazione firewall

- Azione: Seleziona blocco

- Interfaccia: scegliere l'interfaccia a cui si applica la regola
- Famiglia di indirizzi e protocollo: selezionare la voce appropriata
- Origine: lasciare selezionata l'opzione Qualsiasi
- Destinazione: lascia selezionato come Qualsiasi
- Registra: selezionare la casella di controllo per registrare tutti i pacchetti che soddisfano questa regola per l'accounting
- Descrizione: fornire il testo per fare riferimento alla regola in seguito

Selezionare Salva.

Passaggio 5. Esaminare le regole e verificare che la regola di blocco si trovi nella parte inferiore



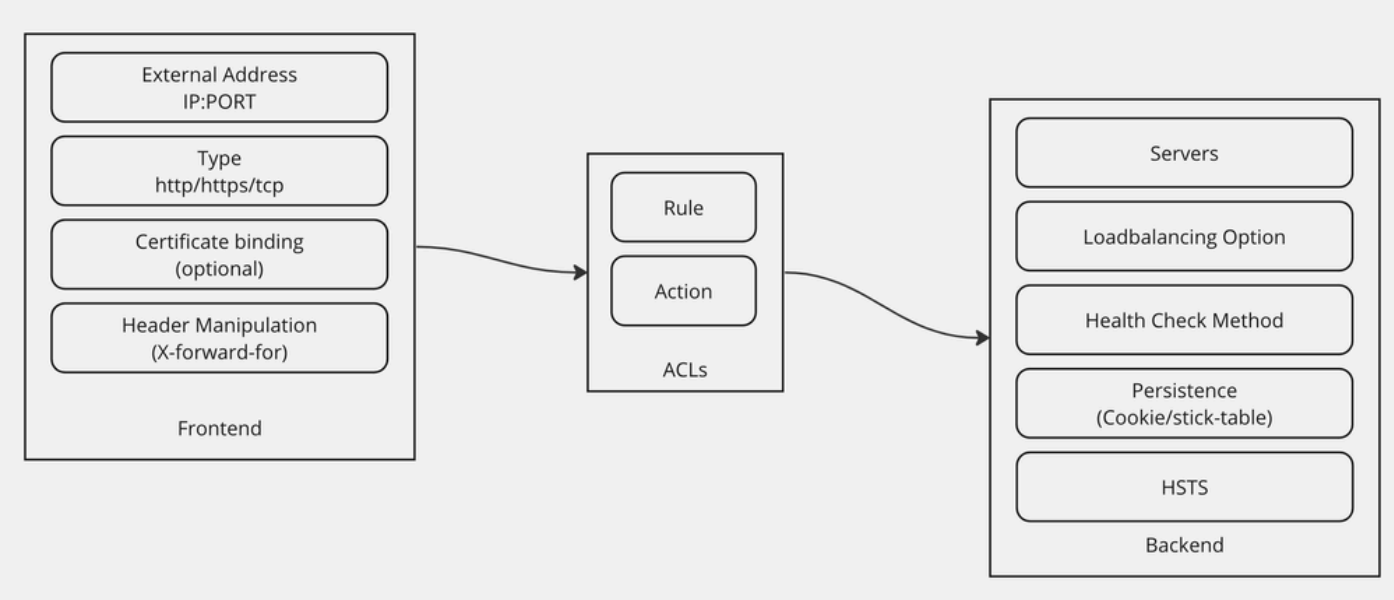
pfSense GUI - Elenco regole firewall

Se necessario, trascinare le regole per ordinarle.

Selezionare Applica modifiche una volta che le regole del firewall sono nell'ordine richiesto per l'ambiente.

Configura HAProxy

Nozioni base su HAProxy



Nozioni base su HAProxy

HAProxy viene implementato con un modello Frontend/Backend.

Il front-end definisce il lato del proxy con cui i clienti comunicano.

Il front-end è costituito da una combinazione di IP e porta, associazione di certificati e può implementare alcune modifiche all'intestazione.

Il back-end definisce il lato del proxy che comunica con i server Web fisici.

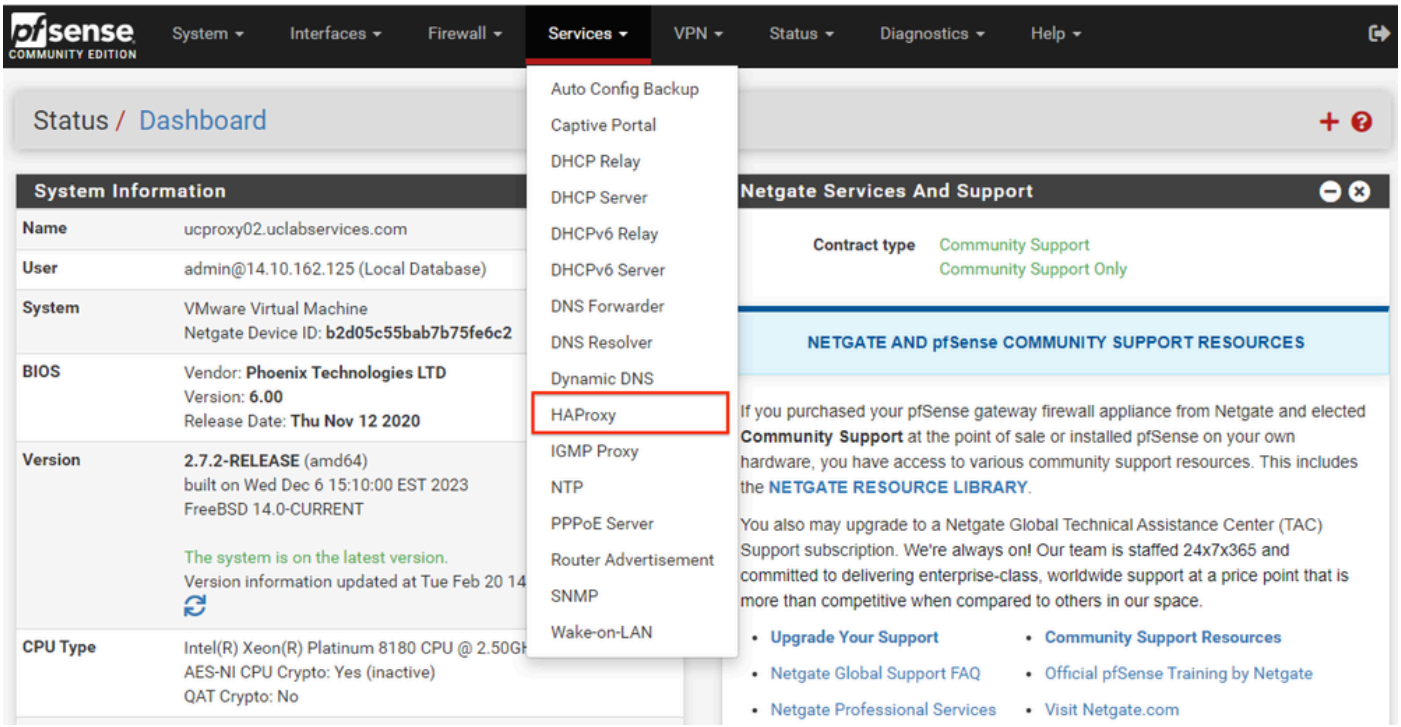
Il back-end definisce i server e le porte effettivi, il metodo di bilanciamento del carico per l'assegnazione iniziale, i controlli di integrità e la persistenza.

Un front-end sa con cosa comunicare il back-end tramite un back-end dedicato o utilizzando gli ACL.

Gli ACL possono creare regole diverse in modo che un dato front-end possa comunicare con back-end diversi a seconda delle esigenze.

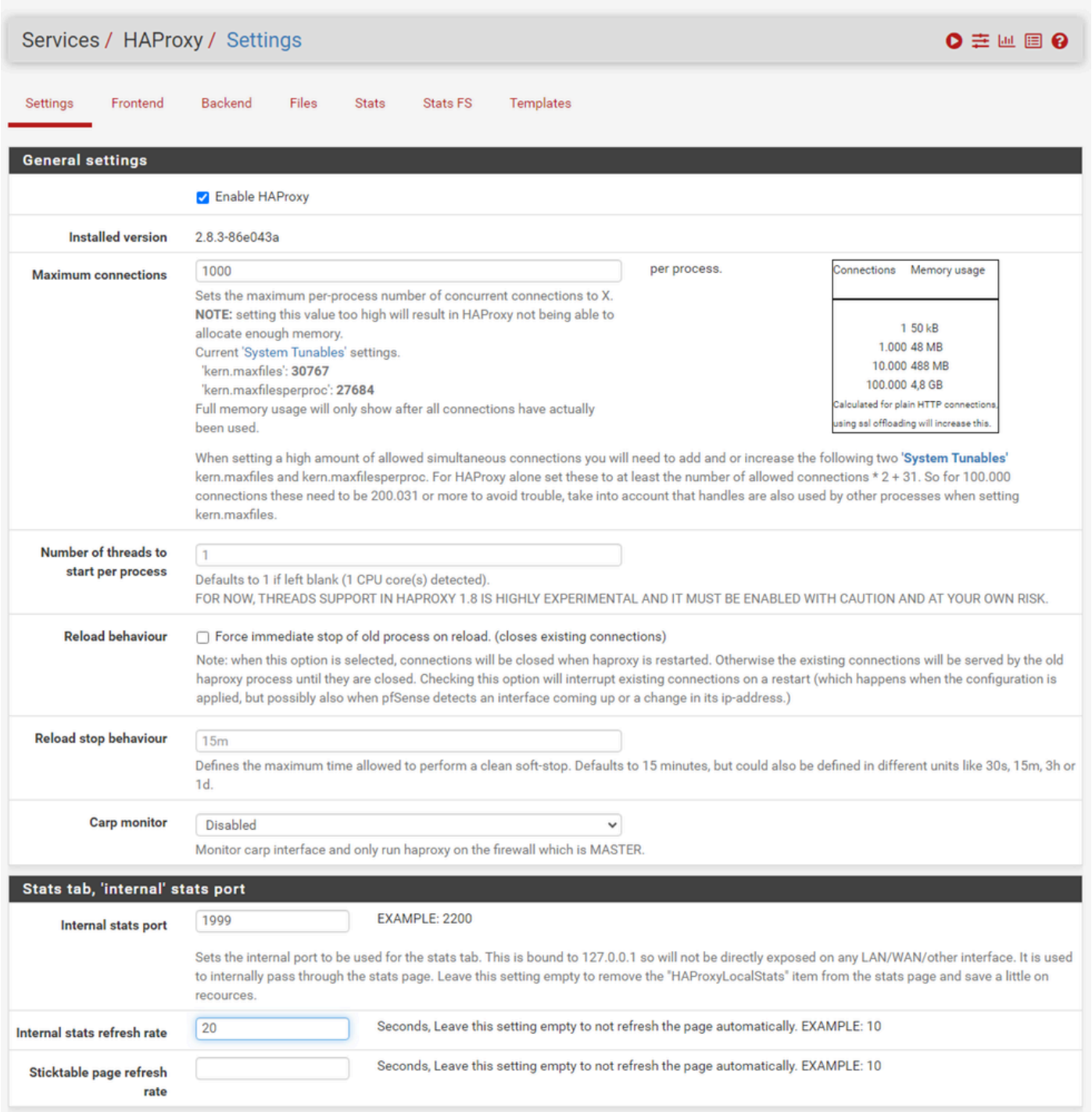
Impostazioni iniziali HAProxy

Passaggio 1. Selezionare HAProxy dall'elenco a discesa Servizi.



GUI pfSense - Elenco a discesa HAProxy

Passaggio 2. Configurare le impostazioni di base



GUI pfSense - Impostazioni principali HAProxy

Selezionare la casella di controllo Abilita HAProxy.

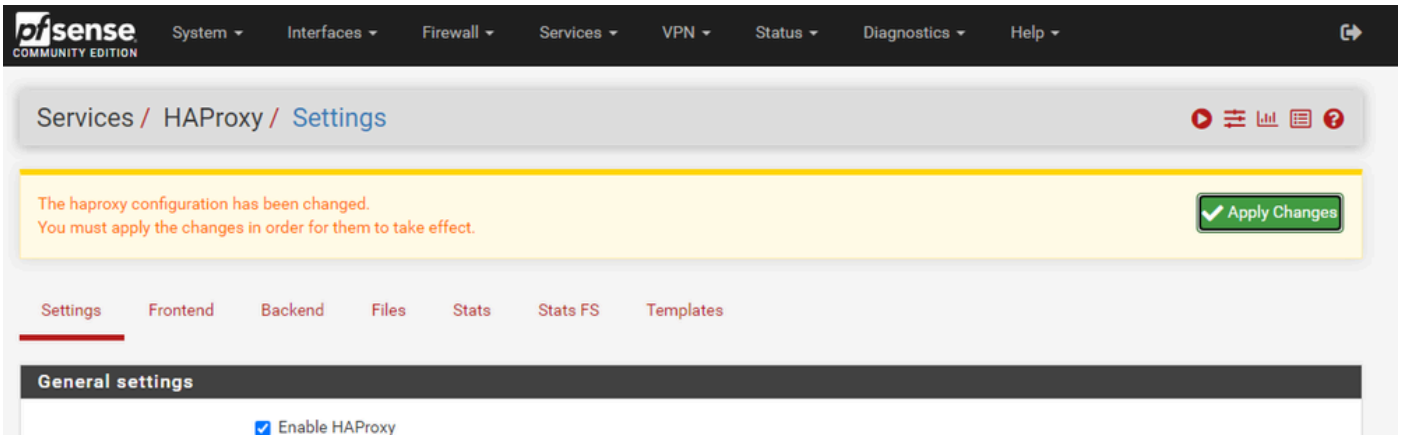
Immettere un valore per Numero massimo di connessioni. Per ulteriori informazioni sulla memoria necessaria, vedere il grafico in questa sezione.

Immettere un valore per la porta Internal Stats. Questa porta viene utilizzata per visualizzare le statistiche HAProxy sull'accessorio, ma non viene esposta all'esterno dell'accessorio.

Immettere un valore per la frequenza di aggiornamento dello stato Interno.

Esaminare la configurazione rimanente e aggiornarla in base alle esigenze dell'ambiente.

Selezionare Salva.

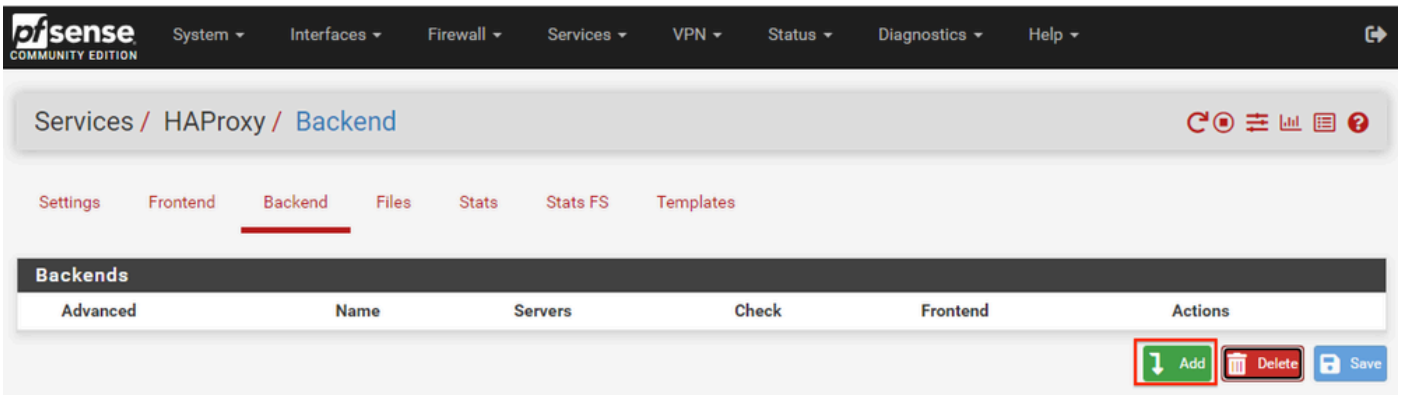


GUI pfSense - Modifiche applicazione HAProxy

Nota: le modifiche alla configurazione non vengono rese attive fino a quando non si seleziona il pulsante Applica modifiche. È possibile apportare più modifiche alla configurazione e applicarle tutte contemporaneamente. Non è necessario applicare la configurazione per utilizzarla in un'altra sezione.

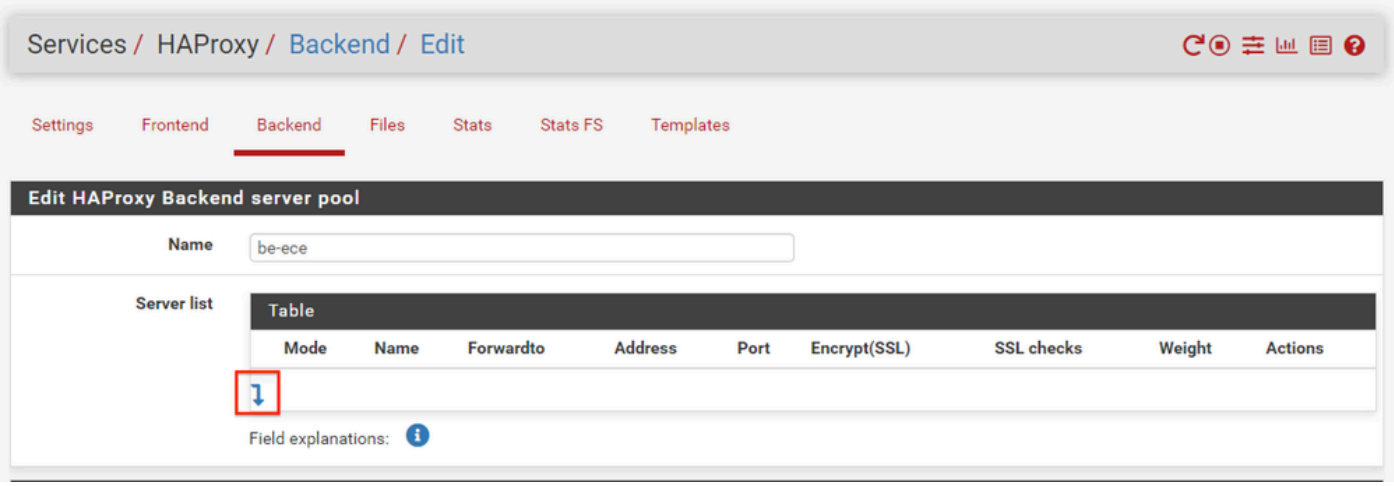
Configura back-end HAProxy

Iniziare con il back-end. Il motivo è che il front-end deve fare riferimento a un back-end. Assicurarsi di aver selezionato il menu Back-end.



pfSense GUI - HAProxy Add Backend

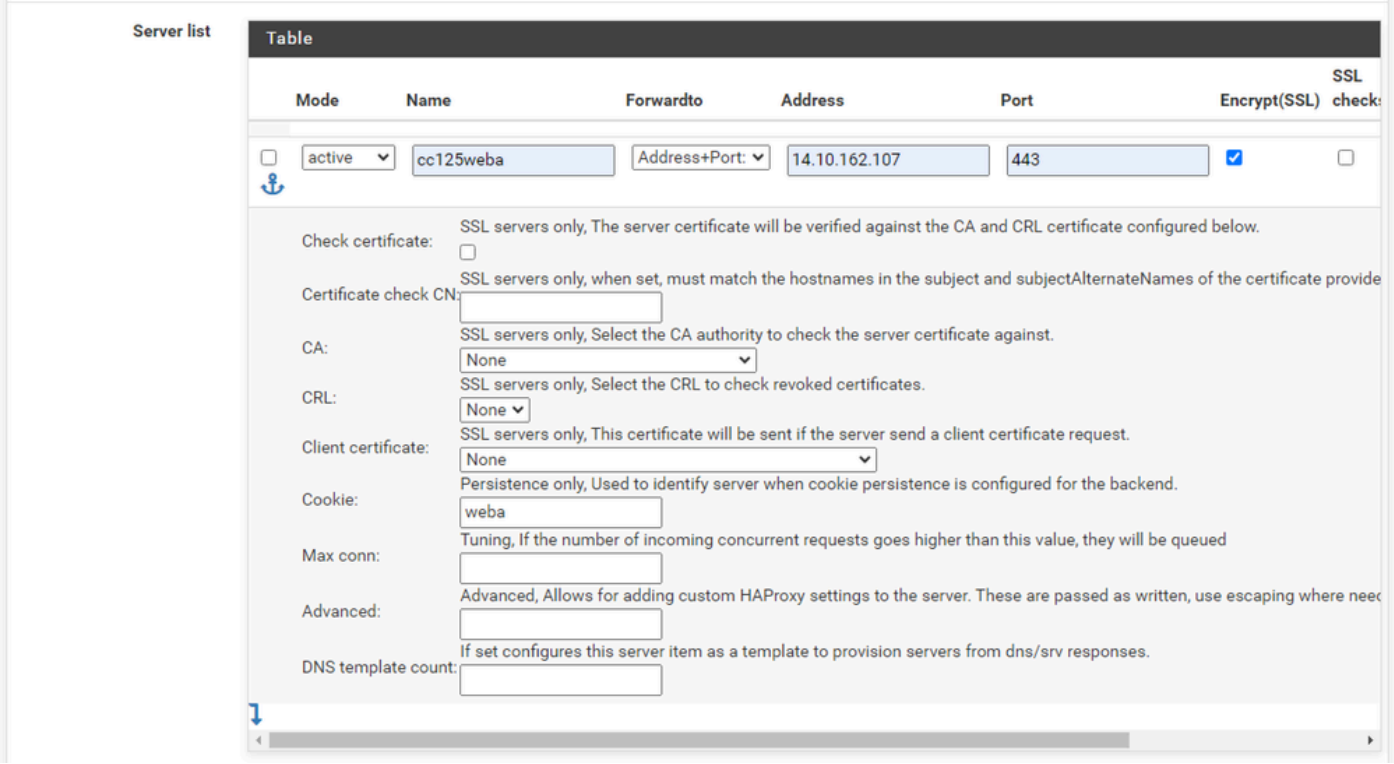
Selezionare il pulsante Aggiungi.



GUI pfSense - Avvio back-end HAProxy

Specificare un nome per il back-end.

Selezionare la freccia rivolta verso il basso per aggiungere il primo server all'elenco Server



Back-end - Elenco server

Specificare un nome per fare riferimento al server. Non è necessario che corrisponda al nome effettivo del server. Questo è il nome visualizzato nella pagina Statistiche.

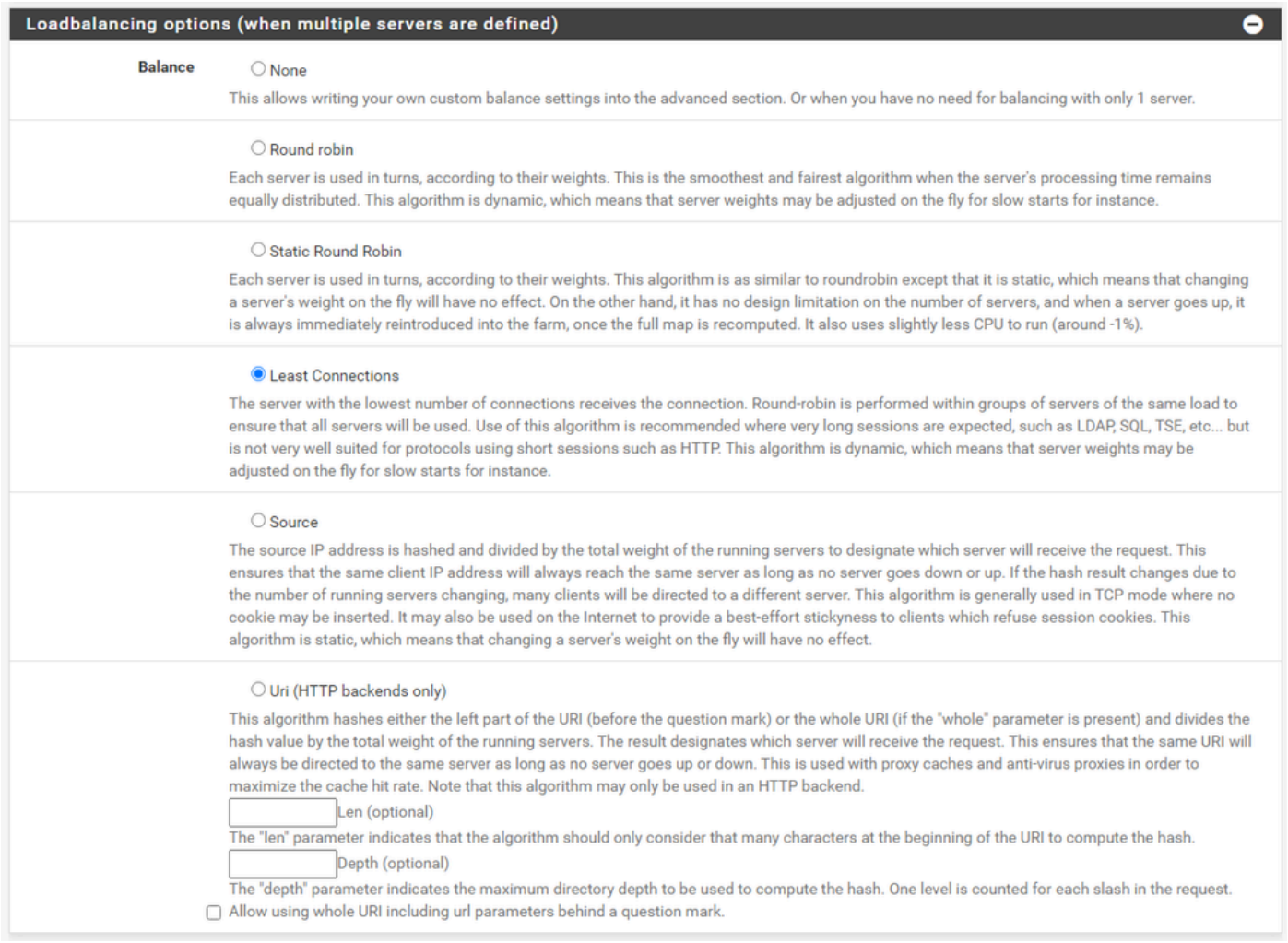
Specificare l'indirizzo del server. Può essere configurato come indirizzo IP per il nome di dominio completo.

Specificare la porta a cui connettersi. Deve essere la porta 443 per ECE.

Selezionare la casella di controllo Encrypt(SSL).

Specificare un valore nel campo Cookie. Questo è il contenuto del cookie di persistenza della sessione e deve essere univoco all'interno del back-end.

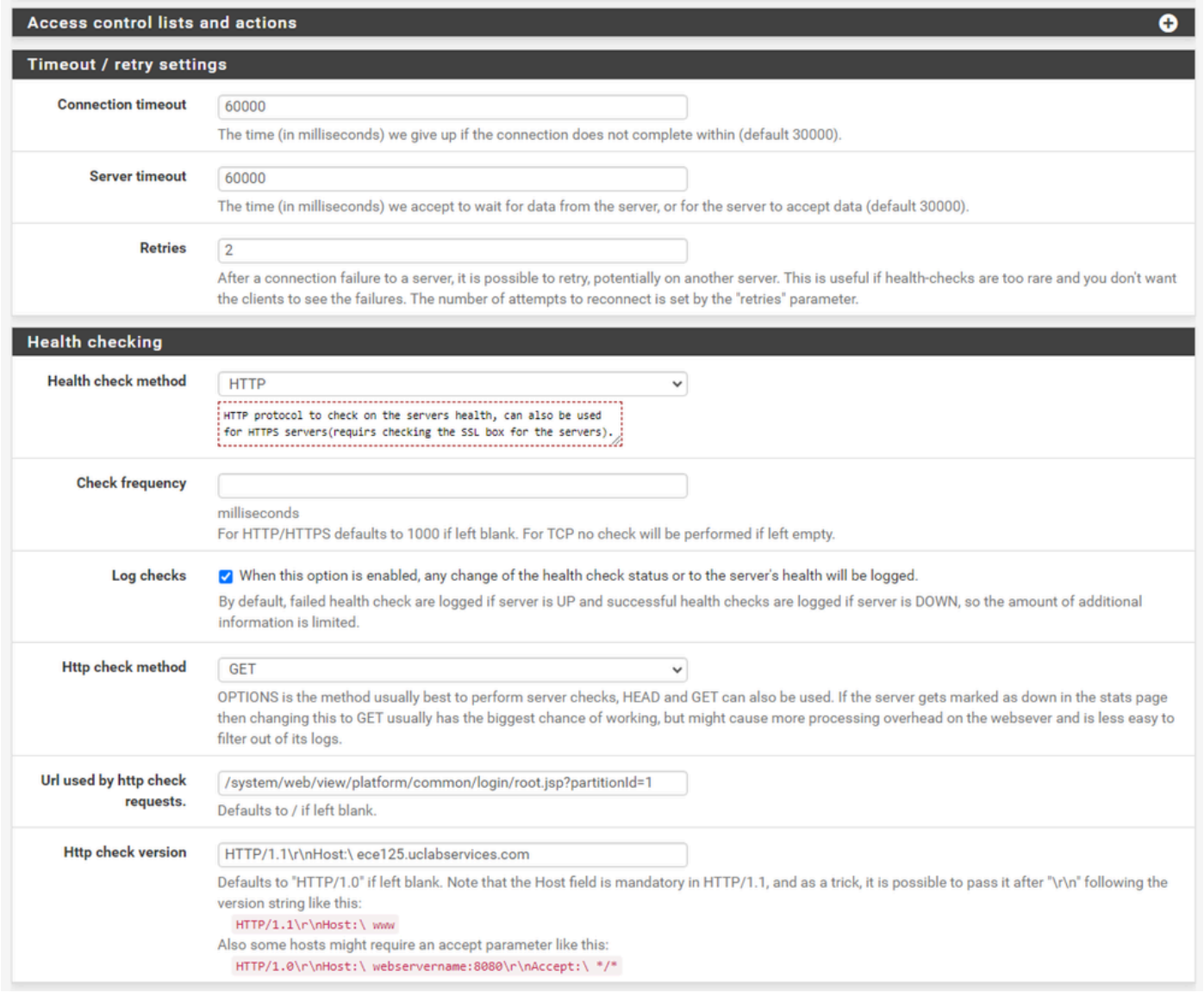
Dopo aver configurato il primo server, selezionare la freccia rivolta verso il basso per configurare altri server Web nell'ambiente.



Back-end HAProxy - Bilanciamento del carico

Configurare le opzioni di bilanciamento del carico.

Per i server ECE, deve essere impostato su Connessioni minime (Least Connections).



Back-end HAProxy - Verifica dello stato

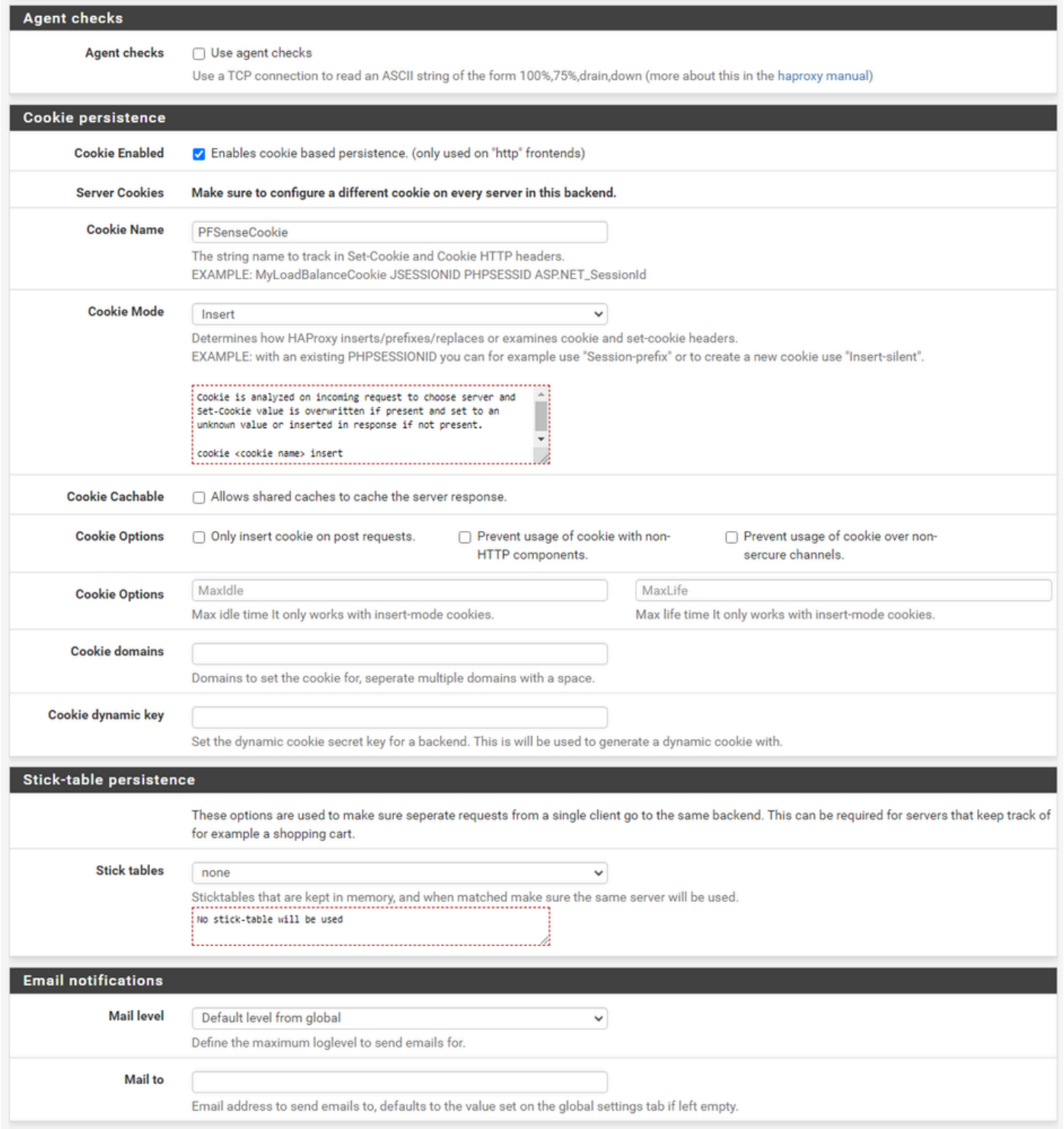
Gli elenchi di controllo di accesso non vengono utilizzati in questa configurazione.

È possibile lasciare le impostazioni di timeout/ripetizione dei tentativi nella configurazione predefinita.

Configurare la sezione di controllo dello stato.

1. Metodo di verifica dello stato: HTTP
2. Frequenza di controllo: lasciare vuoto per utilizzare il valore predefinito ogni 1 secondo.
3. Controlli registro: selezionare questa opzione per scrivere nei registri eventuali modifiche relative allo stato.
4. Metodo di controllo HTTP: selezionare GET dall'elenco.
5. Url utilizzato dalle richieste di controllo HTTP.: Per un server ECE immettere /system/web/view/platform/common/login/root.jsp?partitionId=1
6. Versione controllo HTTP: Invio, HTTP/1.1\r\n\Host:\ {fqdn_of_server}

Assicurarsi di includere uno spazio dopo la barra rovesciata finale ma prima del nome di dominio completo del server.

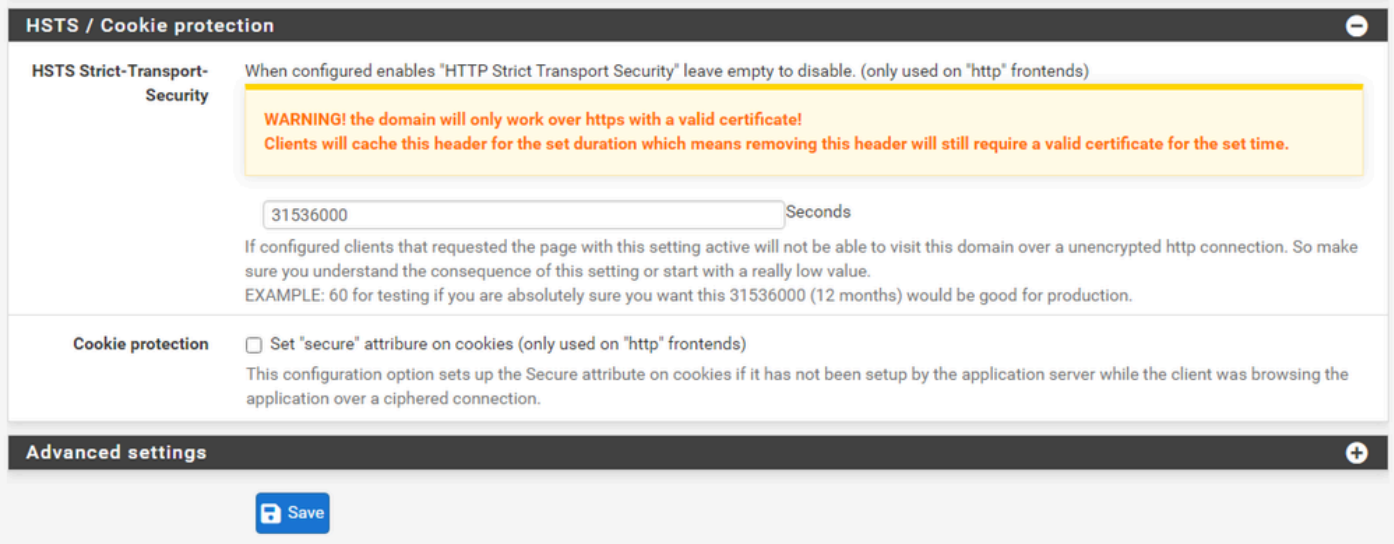


Backend HAProxy - Persistenza cookie

Non selezionare i controlli dell'agente.

Configura persistenza cookie:

1. Cookie abilitato: selezionare questa opzione per abilitare la persistenza basata su cookie.
2. Nome cookie: specificare un nome per il cookie.
3. Modalità cookie: selezionare Inserisci dall'elenco a discesa.
4. Lasciate deselezionate le altre opzioni.



Backend HAProxy - HSTS

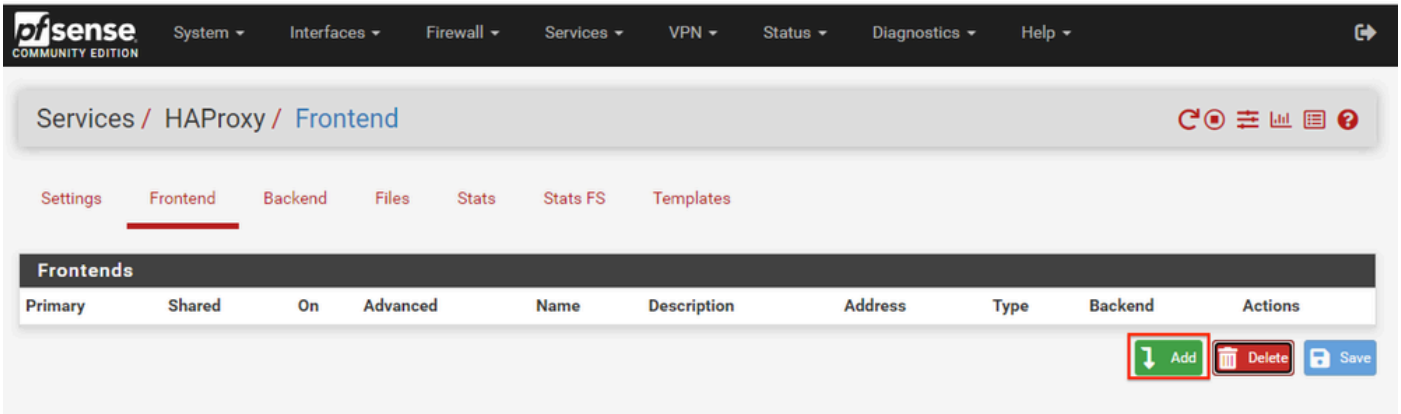
Le sezioni rimanenti del modulo di configurazione back-end possono essere lasciate nelle impostazioni predefinite.

Se si desidera configurare l'host, configurare un valore di timeout in questa sezione. Il modulo ECE inserisce anche un cookie HSTS in modo che questa configurazione sia ridondante.

Selezionare, Salva.

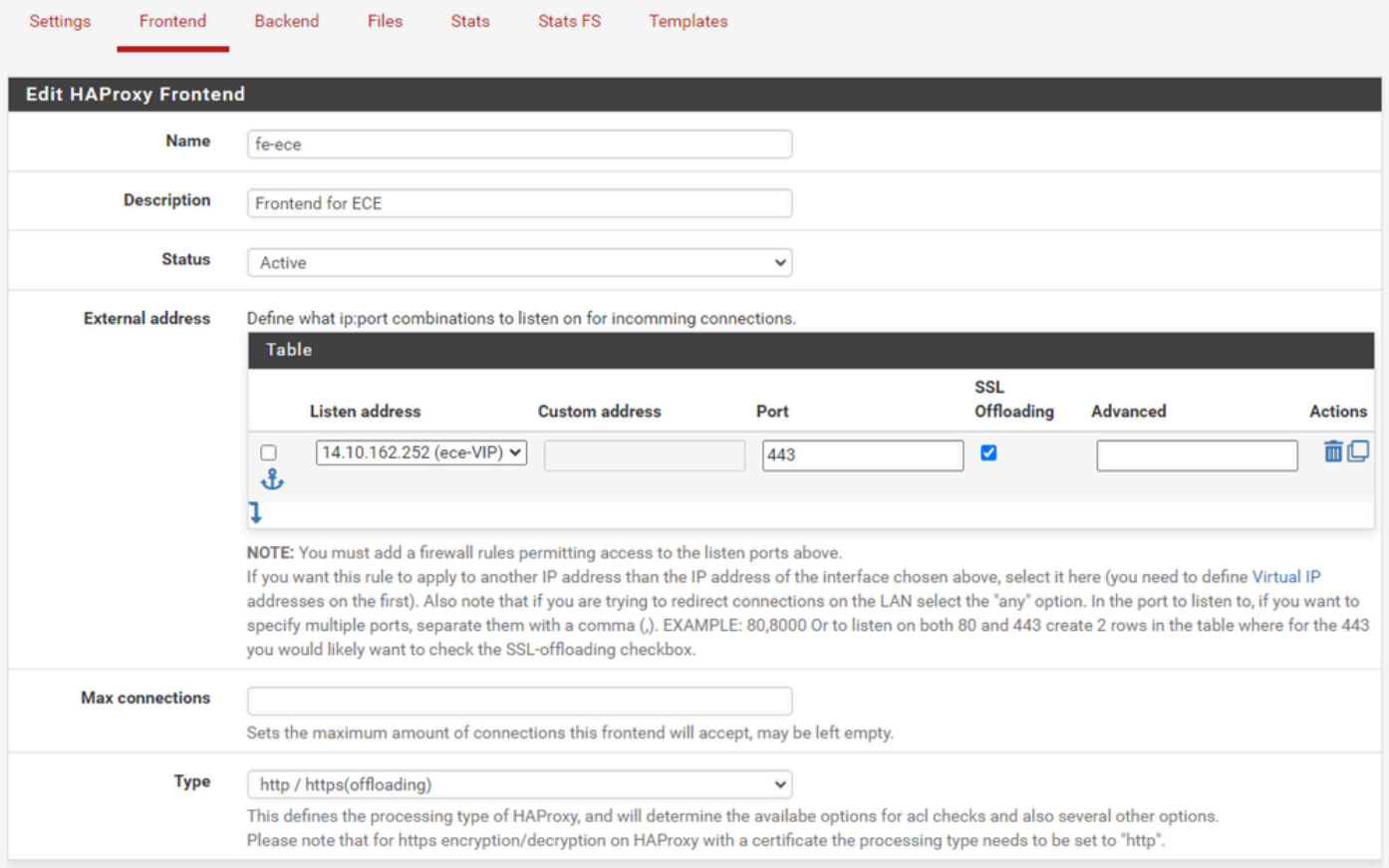
Configura front-end HAProxy

Passate al menu Frontend.



pfSense GUI - HAProxy Add Frontend

Selezionare il pulsante Aggiungi



HAProxy - intestazione front-end

Specificare un nome per il front-end.

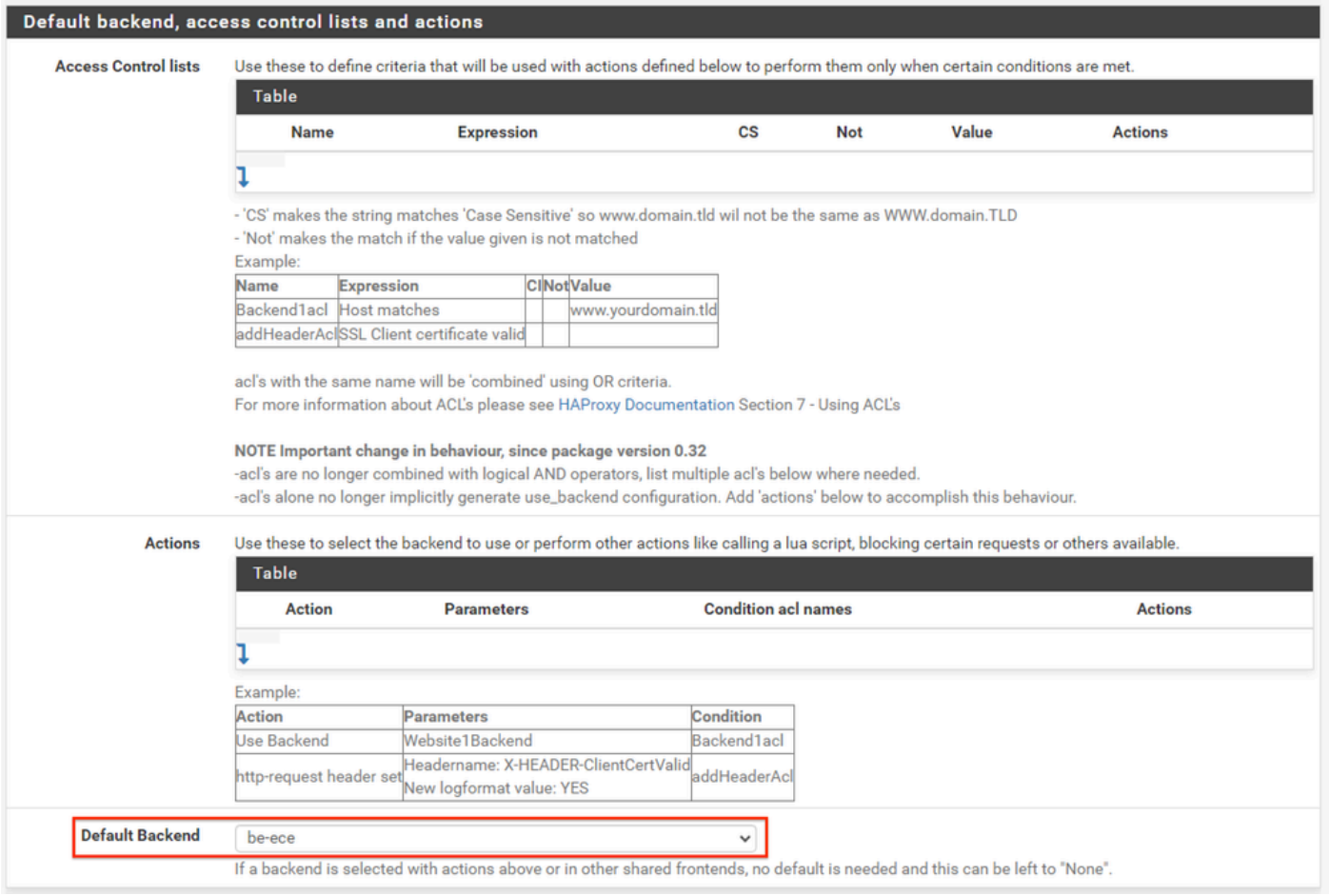
Fornire una descrizione per identificare il front-end in un secondo momento.

Nella tabella Indirizzi esterni:

1. Indirizzo di ascolto: selezionare l'indirizzo VIP creato per il sito Web.
2. Port: immettere 443.
3. Offload SSL: selezionare questa opzione per consentire l'inserimento di un cookie di sessione.

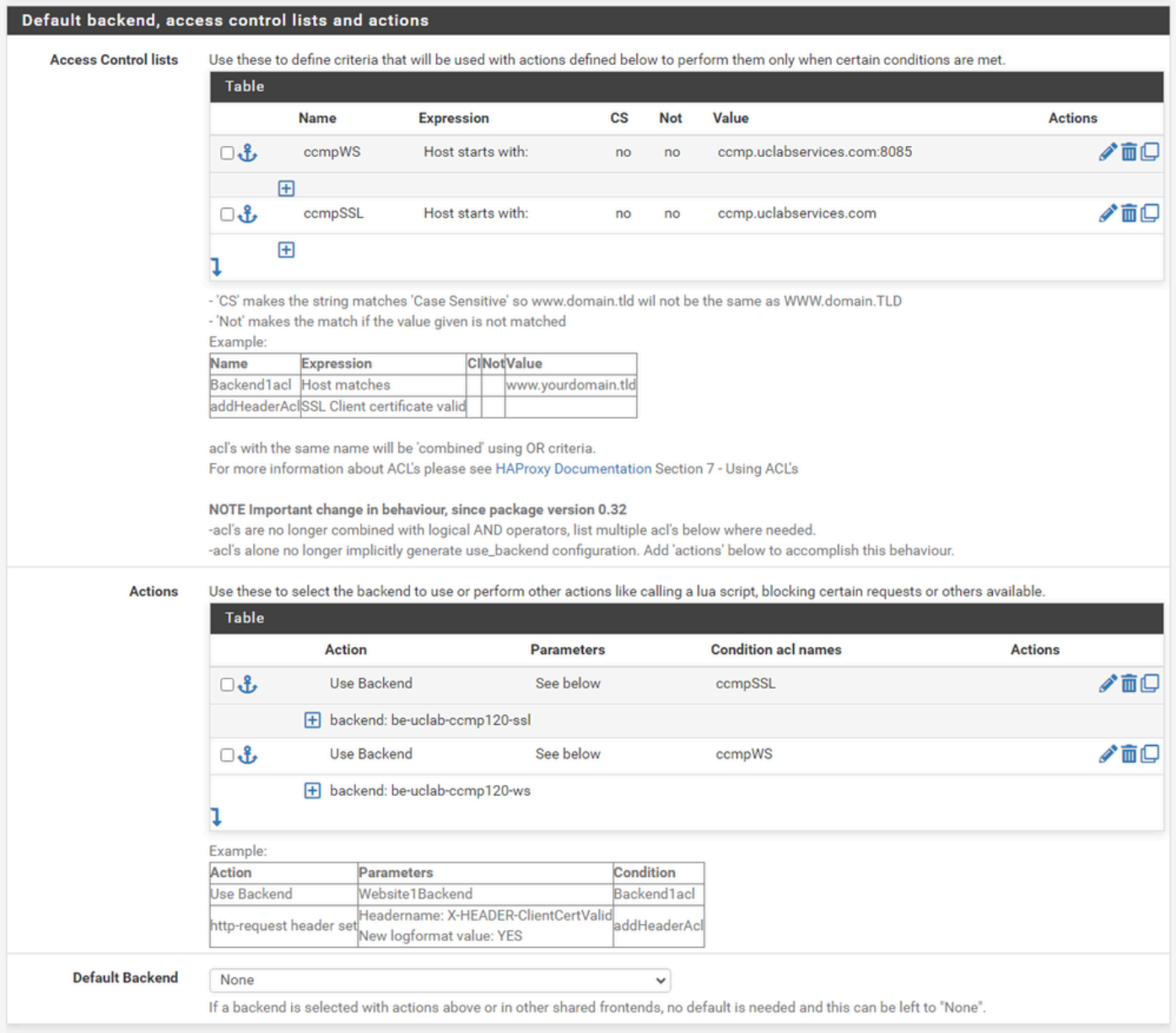
Lasciare vuote le connessioni Max.

Assicurarsi che il Tipo sia selezionato come http / https(offload).



Backend HAProxy - Selezione back-end predefinita

La configurazione più semplice consiste nel scegliere un back-end di default dall'elenco a discesa. Questa opzione può essere selezionata quando l'indirizzo VIP ospita un singolo sito Web.

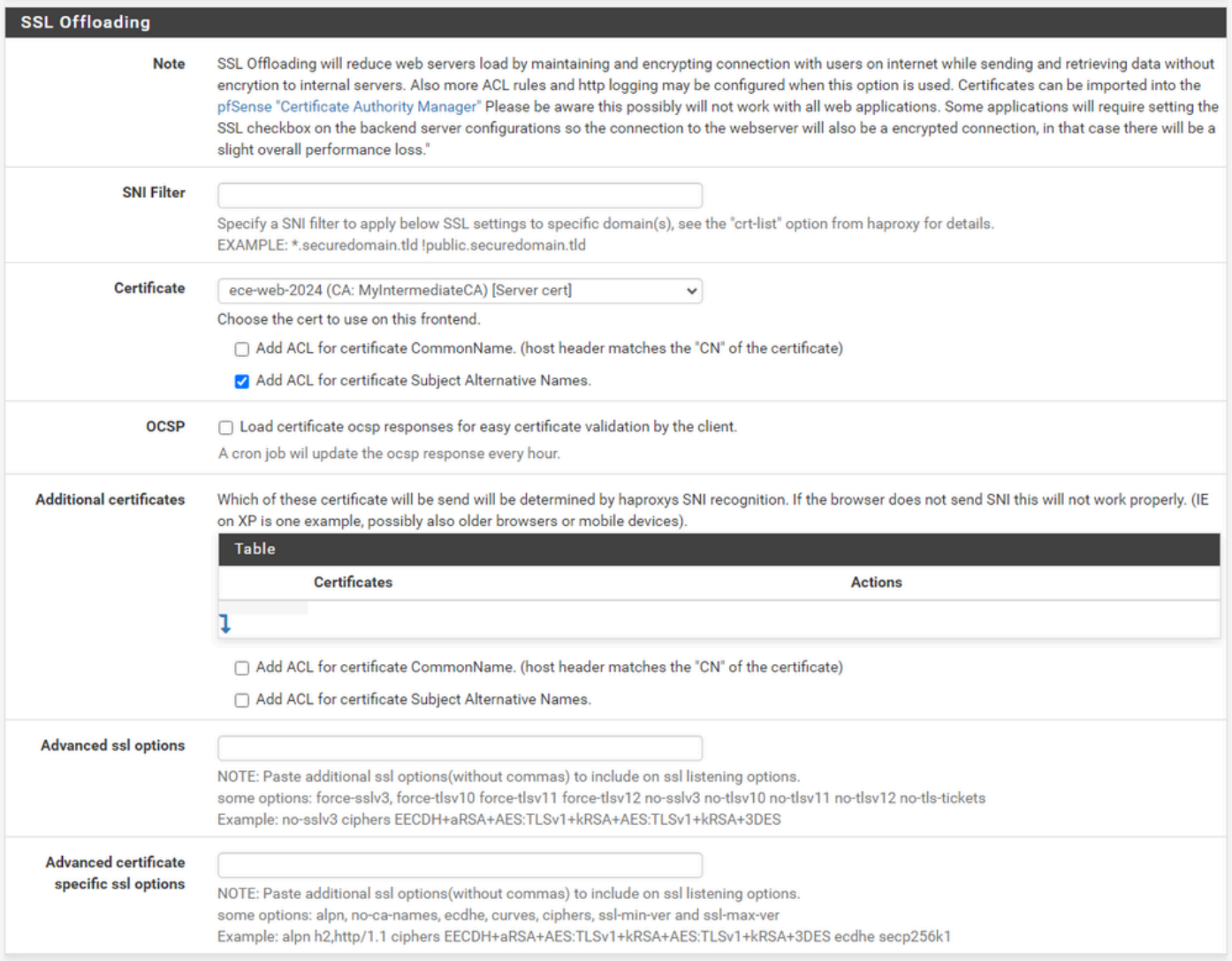


Backend HAProxy - ACL - Avanzate

Come mostrato nell'immagine, gli ACL possono essere usati per reindirizzare un singolo front-end a più back-end in base alle condizioni.

È possibile notare che l'ACL verifica se l'host nella richiesta inizia con un nome e un numero di porta o semplicemente con il nome. In base a questo viene utilizzato un back-end specifico.

Ciò non è comune con l'ECE.



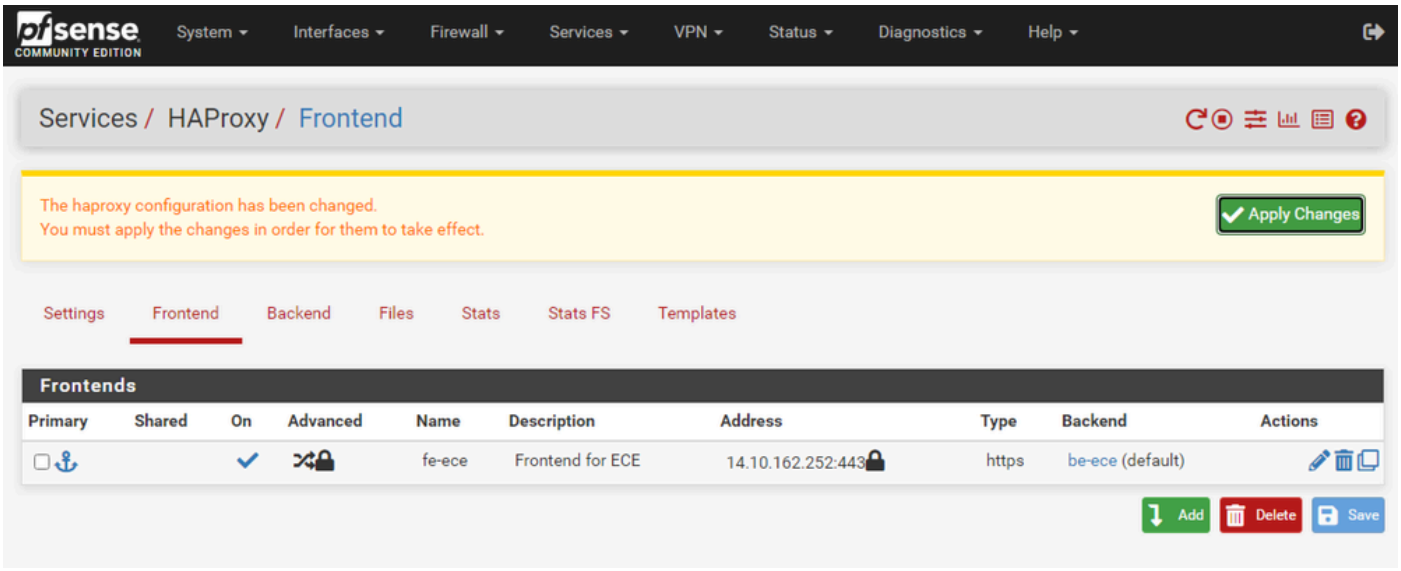
Frontend HAProxy - Associazione certificato

Nella sezione Offload SSL selezionare il certificato creato per l'utilizzo con il sito. Il certificato deve essere un certificato server.

Selezionare l'opzione Add ACL for certificate Subject Alternative Names (Aggiungi ACL per nomi alternativi soggetto certificato).

È possibile lasciare le opzioni rimanenti ai valori predefiniti.

Selezionare, Salva alla fine del modulo.



HAProxy - Applica configurazione

Selezionare Applica modifiche per eseguire il commit delle modifiche di front-end e back-end nella configurazione in esecuzione.

Congratulazioni, hai completato l'installazione e la configurazione di pfSense.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).